

UNITED STATES OF AMERICA  
 DEPARTMENT OF HEALTH AND HUMAN SERVICES  
 FOOD AND DRUG ADMINISTRATION  
 + + +  
 CENTER FOR DEVICES AND RADIOLOGICAL HEALTH  
 PATIENT ENGAGEMENT ADVISORY COMMITTEE

+ + +  
 September 10, 2019  
 8:00 a.m.

Holiday Inn  
 Two Montgomery Village Avenue  
 Gaithersburg, MD 20879

COMMITTEE MEMBERS:

PAUL T. CONWAY	Chair
CYNTHIA L. CHAUHAN, M.S.W.	Committee Member
BENNET R. DUNLAP, M.S.	Committee Member
NECIE EDWARDS	Committee Member
AMYE L. LEONG, M.B.A.	Committee Member
MONICA PARKER, M.D.	Committee Member
MARY (SUZANNE) SCHRANDT, J.D.	Committee Member
RAJIV N. RIMAL, Ph.D.	Temporary Non-Voting Member
KATHERINE D. SEELMAN, Ph.D.	Consumer Representative
MONDIRA BHATTACHARYA, M.D.	Industry Representative
LISA GILBERT	Consultant
PHILIP RUTHERFORD	Consultant
KRISTINA SHERIDAN	Consultant
LETISE WILLIAMS	Designated Federal Officer

*This transcript has not been edited or corrected, but appears as received from the commercial transcribing service. Accordingly, the Food and Drug Administration makes no representation as to its accuracy.*

Free State Reporting, Inc.  
 1378 Cape St. Claire Road  
 Annapolis, MD 21409  
 (410) 974-0947

## FDA REPRESENTATIVES:

NORMAN "NED" SHARPLESS, M.D.  
Acting Commissioner

MICHELLE TARVER, M.D., Ph.D.  
Director, Patient Science & Engagement Program  
CDRH

SUZANNE SCHWARTZ, M.D., M.B.A.  
Deputy Director (& Acting Office Director), Office of Strategic Partnerships and  
Technology Innovation  
CDRH

CHINYELUM OLELE, CDR  
Office of the Commissioner

SANDY WALSH  
Press Contact

## ROUNDTABLE MODERATORS:

HEATHER BENZ, Ph.D., RAC  
Office of Center Director  
CDRH/FDA

ASTIN ROSS, Ph.D.  
FDA

FRASER BOCELL, Ph.D.  
CDRH/FDA

DAVID GEBBEN, Ph.D.  
CDRH/FDA

SUSAN CHITTOORAN  
Patient Affairs Staff  
FDA

ANINDITA SAHA  
Director, External Expertise and Partnerships  
Office of the Center Director  
CDRH/FDA

VICKI MOYER  
CDRH/FDA

MATTHEW HAZLETT  
CDRH/FDA

ALLEN CHEN, Ph.D.  
CDRH/FDA

TAMMY WALLACE  
FDA

MIMI NGUYEN  
External Expertise and Partnerships  
Office of the Center Director  
CDRH/FDA

## PRESENTERS:

SETH D. CARMODY, Ph.D., HCISPP  
Cybersecurity Program Lead  
Office of Strategic Partnerships & Technology Innovation  
CDRH/FDA

KEVIN FU, Ph.D.  
Associate Professor  
University of Michigan

CHRISTIAN DAMEFF, M.D.  
University of California, San Diego

JAY RADCLIFFE  
Thermo Fischer Scientific

JODI DUCKHORN  
Acting Deputy Director, Office of Communication and Education  
CDRH/FDA

CATINA O'LEARY, Ph.D., LMSW  
President/CEO, Health Literacy Media

NASTASSIA TAMARI  
Association Director, Cybersecurity Incident Response  
Becton Dickinson (BD)

KAREN McCHESNEY  
Juvenile Diabetes Research Foundation (JDRF)

## OPEN PUBLIC HEARING SPEAKERS:

VERONICA SCHMITT  
Medical Device Recipient

MARIE MOE  
Medical Device Recipient

ZACH ROTHSTEIN, J.D.  
Vice President, Technology and Regulatory Affairs  
AdvaMed

BENJAMIN WEST  
Medical Device Recipient

NATHANAEL PAUL, Ph.D.  
Medical Device Recipient

GRETCHEN RICCARDI  
Medical Device Recipient

REID D'AMICO, Ph.D.  
Medical Device Recipient

BEAU WOODS  
Cyber Safety Advocate  
I Am The Cavalry

ANDY CORAVOS  
Co-Founder/CEO, Elektra Labs

NINA ALLI, M.S., USMC  
Executive Director, Biohacking Village  
DEF CON

## OPEN PUBLIC COMMENTER:

KEN HOYME, M.S.E.E.  
Director, Product Security  
Boston Scientific

## INDEX

	PAGE
CALL TO ORDER - Paul T. Conway	9
CONFLICT OF INTEREST STATEMENT - Letise Williams	13
COMMITTEE INTRODUCTIONS	18
WELCOME AND OPENING REMARKS - Norman "Ned" Sharpless, M.D.	21
UPDATES FROM THE CDRH PATIENT SCIENCE & ENGAGEMENT PROGRAM - Michelle Tarver, M.D., Ph.D.	27
MEDICAL DEVICE CYBERSECURITY: A TOTAL PRODUCT LIFECYCLE APPROACH - Seth D. Carmody, Ph.D., HCISPP	29
CYBERSECURITY AND MEDICAL DEVICE UPDATES - Kevin Fu, Ph.D.	34
PHYSICIAN PERSPECTIVE ON CYBERSECURITY - Christian Dameff, M.D.	39
CYBERSECURITY VULNERABILITIES - Jay Radcliffe	45
CDRH COMMUNICATION OF MEDICAL DEVICE VULNERABILITIES AND SAFETY CONCERNS - Jodi Duckhorn	49
CYBERSECURITY VULNERABILITY COMMUNICATION - Catina O'Leary, Ph.D., LMSW	56
INDUSTRY PERSPECTIVE ON CYBERSECURITY COMMUNICATION - Nastassia Tamari	64
PATIENT PERSPECTIVE ON CYBERSECURITY COMMUNICATION - Karen McChesney	69
QUESTIONS BY THE COMMITTEE	73

## INDEX

	PAGE
OPEN PUBLIC HEARING	
Veronica Schmitt (video)	84
Marie Moe (video)	88
Zach Rothstein, J.D.	90
Benjamin West	92
Nathanael Paul, Ph.D.	93
Gretchen Riccardi	96
Reid D'Amico, Ph.D.	98
Beau Woods	101
Andy Coravos	103
Nina Alli, M.S., USMC	106
QUESTIONS BY THE COMMITTEE	107
ROUNDTABLE DISCUSSIONS	125
ROUNDTABLE SUMMATIONS	126
OPEN PUBLIC COMMENT	141
OPEN COMMITTEE DISCUSSION	143
COMMITTEE DISCUSSION OF FDA QUESTIONS	
Question 1	155
Question 2	166
Question 3	177
Question 4	187
Question 5	198

## INDEX

	PAGE
CLOSING REMARKS	
Suzanne Schwartz, M.D., M.B.A.	208
Michelle Tarver, M.D., Ph.D.	209
Paul T. Conway	209
ADJOURNMENT	210



MEETING

(8:00 a.m.)

MR. CONWAY: Good morning, and welcome to the third meeting of the Food and Drug Administration's Patient Engagement Advisory Committee, known by many as the PEAC or PEAC.

My name is Paul Conway, and I have the distinct honor to serve the public, the FDA, and my fellow Advisory Committee members as the Chair of this Committee. I formally call this meeting to order.

As our public audience here in Gaithersburg, Maryland finishes taking their seats, the Committee would like to extend a warm welcome to those in the room today who have joined us as well as those across America and beyond who will be watching our proceedings via our live webcast. We both respect and appreciate your attention to our Committee and the time you have invested to engage with us today.

At this point, I'd like to note for the record that the non-voting members constitute a quorum as required by 21 C.F.R. Part 14. I'd also like to add that the Committee members participating in today's meeting have received training in FDA device law and regulation.

Beyond my service as Chair of this Committee, I had the privilege to serve as Chair of Policy and Global Affairs for the American Association of Kidney Patients, the largest and oldest independent kidney patient organization in the United States. I'm a patient who has managed kidney disease for nearly 50 years, including 13 years of chronic kidney disease, nearly 3 years on dialysis through a home-based device, and for the past 23 years as the fortunate recipient of a kidney from a courageous young teenage organ donor whose life was cut short. His gift of life to me, made sustainable through an astounding array of devices, diagnostics, and biologics, has afforded me a new life and the opportunity to continue a career marked by public service.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Professionally, my background is in state and federal government policy implementation, including direct experience with the creation and standup of the U.S. Department of Homeland Security in the aftermath of September 11th, 2001.

Before my fellow Committee members introduce themselves, it is both important and relevant to relay our history over the previous 3 years and to briefly restate our official Committee charge from the FDA. Later Dr. Michelle Tarver will discuss our impacts.

The PEAC is an FDA Advisory Committee, which is the most formal and public method by which the FDA obtains independent expert advice on scientific, technical, and policy matters. In essence, the PEAC is one of the most direct ways that the public can provide comments and key recommendations to the FDA. This Committee was initiated proactively by FDA based on the foresight of FDA leadership and with wide support and valuable insights offered by patients, caregivers, and multiple other stakeholders engaged in the medical research and device development cycle.

For this Committee, the path from concept to standup was an immensely complex undertaking because regulatory agencies like the FDA that are charged with protecting public safety and shepherding the approval of medical innovations must operate within a well-established body of laws and regulations that determine how expert insights and recommendations are actually gathered by the federal government. These safeguards ensure public trust between citizens and their government is maintained and that agency professionals glean relevant information without any appearance or actual undue influence or to the perceived advantage of any person or entity.

The standup of the PEAC was a bold move and a very clear signal to all stakeholders involved in the medical device development process that patient life experiences, including preferences and insights gained from suffering and burden, are both valued and valuable to decision makers. The FDA action is fully consistent and supported by similar efforts across

the federal government and the U.S. Congress to better engage patients in precision medicine, patient-driven quality measures, patient-reported outcome data, and real-world experiences.

Our first PEAC meeting was conducted in October of 2017 and was entitled "Patient Engagement and Medical Device Clinical Trials." At this meeting, Committee members listened and discussed substantive expert testimony and public comments related to various aspects of patient engagement in clinical trial design, including safety concerns and risk tolerance, other issues related to the approval, regulation, and payment of new medical devices.

Our second PEAC meeting conducted in November of 2018 was entitled "Connected and Empowered Patients: E-Platforms Potentially Expanding the Definition of Scientific Evidence." At this meeting, Committee members listened and deliberated expert opinion and public testimony related to patient-generated health data, including social media, sensor data, and patient-driven registries, and how to better engage patients and consumers as empowered partners in the work of protecting public health and promoting responsible innovation.

For today, our third PEAC meeting, our agenda is entitled "Cybersecurity and Medical Devices: Communication that Empowers Patients," and the Committee will once again hear formal testimony, public comment, and conduct a related discussion on potential recommendations. These recommendations will address which factors should be considered by FDA and industry when communicating cybersecurity risk to patients and to the public, including but not limited to the content, phrasing, and methods used to disseminate the message and the timing of that communication. The recommendations will also address concerns patients have about changes to their devices to reduce cybersecurity risks, as well as the role of other stakeholders, such as healthcare providers, in

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

communicating cybersecurity risks to patients.

For the public, and especially for our fellow patient/consumers who are listening to these proceedings today, you should know that the work of this Committee and our ongoing substantive engagement with FDA officials extends far beyond merely attending meeting dates and getting set for these events. For example, since November of 2018, PEAC Committee members have been engaged with FDA officials in a series of homework assignments that touched directly on strategic priorities as well as expounding on topics brought up during the in-process meeting. FDA has been highly interested in the opinions of commissioners and Committee members and have actively sought out our insights and perspectives on a host of issues related to both PEAC operations and future areas of review and deliberation.

I will now read into the record the precise purpose of the PEAC, which is available online on the FDA website. Stating our purpose at the outset provides an important context in advance of our discussions and for future transcripts so that it is absolutely clear what the PEAC is and what the PEAC is not.

The Committee provides advice to the Commissioner or designee on complex issues relating to medical devices, the regulation of devices, and their use by patients. The Committee may consider topics such as Agency guidance and policies, clinical trial or registry design, patient preference study design, benefit-risk determinations, device labeling, unmet clinical needs, available alternatives, patient-reported outcomes, and device quality of life or health status issues and other patient-related topics. The Committee will provide relevant skills and perspectives in order to improve communication of benefits, risks, clinical outcomes, and increase integration of patient perspectives into the regulatory process for medical devices. It will perform its duties by discussing and providing advice and recommendations in ways such as identifying new approaches,

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

promoting innovation, recognizing unforeseen risk or barriers, and identifying unintended consequences that could result from FDA policy.

My fellow Committee members are serious individuals who are driven by a shared sense of purpose and a genuine desire to serve their country and patients through the mission of this Committee and in their many other roles. They do not presume to speak for all patients and they are not on this Committee as an advocate or champion of any particular viewpoint, organization, or industry. Instead, they are here to advance the public good and to aid the FDA in their ongoing commitment to view patients as experts, to substantively include patient expertise and their experiences within FDA deliberations.

On behalf of the full Committee, I'd like to again thank the leadership and the career civil servants of the FDA for your public service, for the establishment of the PEAC, and for honoring the mission to engage patients and respect their insights over the course of the past 3 years.

Now I'd like to take a few minutes and ask our distinguished fellow Committee members and FDA staff -- let me say this again, I apologize. If you have not signed in at the front table, please do so. It's very important for us to capture that.

And now, actually, what I'd like to do is ask Ms. Letise Williams to go ahead, she's our Designated Federal Officer, and read a few things into the record, and then we'll go ahead and have our fellow commissioners and Committee members introduce themselves.

MS. WILLIAMS: Thank you, Paul. Good morning. I will now read the FDA Conflict of Interest Disclosure Statement.

The Food and Drug Administration (FDA) is convening today's meeting of the Patient Engagement Advisory Committee under the authority of the Federal Advisory Committee Act (FACA) of 1972. With the exception of the Industry Representative, all members of this Committee serve as special Government employees and are subject to Federal conflict of

interest laws and regulations.

The following information on the status of this Committee's compliance with Federal ethics and conflict of interest laws covered by, but not limited to, those found at 18 U.S.C. 208 are provided to participants in today's meeting and to the public.

FDA has determined that members and consultants of this Committee are in compliance with the Federal ethics and conflict of interest laws. Under 18 U.S.C. 208, Congress has authorized FDA to grant waivers to special Government employees and regular Federal employees who have financial conflicts when it is determined that the Agency's need for a particular individual's services outweighs his or her potential financial conflict of interest.

Related to the discussions of today's meeting, members and consultants of this Committee who are special Government employees have been screened for potential financial conflicts of interest of their own as well as those imputed to them, including those of their spouses or minor children and, for the purposes of 18 U.S.C. 208, their employers. The interests may include investments; consulting; expert witness testimony; contracts/grants/CRADAs; teaching/speaking/writing; patents and royalties; and primary employment.

For today's agenda, the Committee will address cybersecurity and medical devices communication that empowers patients. The recommendations provided by the Committee will address which factors should be considered by FDA and industry when communicating cybersecurity risks to patients and to the public, including but not limited to the content, phrasing, the methods used to disseminate the message, and the timing of that communication. The recommendations will also address concerns patients have about changes to their devices to reduce cybersecurity risks as well as the role of stakeholders, such as healthcare providers, in communicating cybersecurity risks to patients.

Based on the agenda for today's meeting and all financial interests reported by the

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Committee members and consultants, no conflict of interest waivers have been issued in accordance with 18 U.S.C. 208.

Dr. Mondira Bhattacharya is serving as the Industry Representative for communication of benefit and risk information to patients and is acting on behalf of all related industry. She is employed by MyoKardia, Incorporated.

For the record, the Agency notes that Dr. Kevin Fu, who is an invited guest speaker with us today, has acknowledged a financial interest with a firm that manufactures medical devices that have the potential for cybersecurity risks, in the form of scientific advisory board services.

We would like to remind members and consultants that if the discussions involve any other products or firms not already on the agenda for which FDA participants have a personal or imputed financial interest, the participants need to exclude themselves from such involvement and their exclusion will be noted for the record. FDA encourages all other participants to advise the Committee of any financial relationships that they may have with any firms at issue.

A copy of this statement will be available for review at the registration table during this meeting and will be included as part of the official transcript. Thank you.

For the duration of the Patient Engagement Advisory Committee meeting on September 10th, 2019, Dr. Rajiv Rimal has been appointed to serve as a Temporary Non-Voting Member. For the record, Dr. Rajiv Rimal serves as a member of the Risk Communication Advisory Committee in the Office of Special Medical Programs. Dr. Rimal is a special Government employee who has undergone the customary conflict of interest review and has reviewed the material to be considered at this meeting.

This appointment was authorized by Russell Fortney, Director, Advisory Committee Oversight and Management Staff, on August 19th, 2019.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Before I turn the meeting back over to Mr. Conway, I'd like to make a few general announcements.

Transcripts of today's meeting will be available from Free State Court Reporting, Incorporated, located at 1378 Cape St. Claire Road, Annapolis, Maryland 21409. Telephone number: (410) 974-0947.

Information on purchasing videos of today's meeting can be found on the table outside the meeting room.

The press contact for today's meeting is Ms. Sandy Walsh.

I would like to remind everyone that members of the public and the press are not permitted in the Committee area, which is beyond the speaker's podium. I request that reporters please wait to speak to FDA officials until after the Committee meeting has concluded.

If you are presenting in the Open Public Hearing session today and have not previously provided an electronic copy of your slide presentations to FDA, please arrange to do so with Ms. AnnMarie Williams or Mr. Artair at the registration desk.

In order to help the transcriptionist identify who is speaking, please be sure to state your name each and every time that you speak.

For the record, FDA has received zero written comments.

If anyone in the audience has questions or need assistance, please see an FDA representative. FDA staff members are wearing name tags. If anyone has any health or safety concerns, please see one of the FDA representatives with the name tags, and they will be happy to assist you.

This morning when you signed in at the registration desk, you were asked to pull a piece of paper out of a bowl. That paper identifies the table at which you will sit during the 1:00 p.m. roundtable discussion. The purpose of the table assignment is to help create a

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



balance of different perspectives such as industry, academic, and patients at each of the tables. If you wish to participate in the roundtable discussion, we ask that you sit at your assigned table when you return from lunch.

Participation at the roundtable discussion is voluntary. If you do not wish to participate, you are free to sit in one of the chairs located in the back of the room during this portion of the meeting. If you are not participating in the roundtable discussion, you will have an opportunity to make brief comments on the designated topics during the Open Public Comment portion of the meeting. Please note that the roundtable discussion, the webcast will not be available. The webcast will reopen at 2:00 p.m. for the roundtable summations.

Finally, please silence your cell phones and other electronic devices at this time.

Thank you very much.

I will now turn the meeting over to the Chair, Mr. Conway.

MR. CONWAY: Thank you, Letise Williams, Designated Federal Officer and chief principal for keeping the trains running on time and assistance with me. Thank you very much.

At this time, let me go ahead and do a brief recap before we introduce FDA staff and Committee members of today's events. Before we ask FDA to begin with their opening remarks, here's an overview of how today's meeting will run.

During the morning we'll have presentations from FDA, healthcare providers, and industry and patient organizations, followed by open committee discussion. Next, we will break for about 10 minutes. We will reconvene with the Open Public Hearing. After the Open Public Hearing concludes, we will break for lunch at approximately 12:15 p.m. The public will have 45 minutes for lunch. When the public reconvenes from lunch, I will open the meeting for open public discussion. During the open public discussions, I will invite you,

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

the audience, to participate in these roundtable discussions during which you can comment on the scenario that was provided when you signed this morning as well as the scenarios posted on the FDA website. Your participation in these discussions are also completely voluntary, as just indicated by Ms. Williams.

FDA staff will serve as moderators and note takers during these discussions and will provide the table members with the ground rules for commenting. FDA staff will not be providing their thoughts or comments regarding the scenario. Instead, they will be summarizing the comments made by the public at the tables. Please note that the Committee members will not be present during the portion of this open public discussion. The Committee members will return approximately 10 minutes before the scenario discussion concludes. FDA members will then summarize the table discussions for the Committee.

After the Committee discussions, we will have a 15-minute Open Public Comment to give you, the public, an opportunity to comment on the roundtable discussions that you just heard about the scenario. Individuals who would like to comment on the roundtable discussions will be asked to line up at the microphone in the middle of the room and will be given 2 minutes for comments. We'll ask that you respect your fellow attendees by adhering to the time limit for the comments.

Once the open public comments conclude, the Committee will then have an opportunity to discuss all of the comments reported and presented. Afterwards, we'll break for about 15 minutes and return for Committee discussion of the FDA questions. Following our discussion of these questions, I will give closing remarks.

At this point, let me go ahead and start on my right-hand side and have FDA staff introduce themselves, as well as Committee members.

DR. TARVER: Michelle Tarver, Director of Patient Science and Engagement at CDRH.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

DR. SCHWARTZ: Suzanne Schwartz, Acting Director of the Office of Strategic Partnerships and Technology Innovation at CDRH.

MR. DUNLAP: Bennet Dunlap.

MS. EDWARDS: Necie Edwards.

MR. CONWAY: All right, let me just say this, and I apologize. If we could go back to Bennet, just state your affiliation, if you could.

MR. DUNLAP: Oh, excuse me. I've been a diabetes advocate. I have a master's in health communication.

MS. EDWARDS: Necie Edwards. I'm a healthcare advocate, and my specialty is pain management. I have fibromyalgia and ankylosing spondylitis, and I'm very passionate about helping other people with chronic pain.

(Microphone malfunction.)

DR. SEELMAN: I'm Kate Seelman. I want to thank the FDA and its staff, and I'm honored to serve on the Committee in an agency that has such a sterling background in science and now enriched by experience and patients' involvement. My own background, I'm emerita at the University of Pittsburgh in rehabilitation science. I served with the World Health Organization and with the World Bank. I guess you could just say I've been around. But one of the things that interests me is not too long ago somebody -- I've worn hearing aids all my life because I've had very little hearing. Somebody asked me if they were a connected device and whether indeed I was on the internet, so there are many relevant areas here today, and I'm very much appreciative to be a part of the discussions. Thank you.

MS. GILBERT: I'm Lisa Gilbert. I am a cybersecurity instructor for the Air Force through Applied Research Solutions, and I have a daughter with an implanted medical device, a neurostimulator.

DR. RIMAL: I'm Rajiv Rimal. I'm a professor at the Johns Hopkins School of Public Health.

MR. RUTHERFORD: I'm Phil Rutherford, and I'm a recovery advocate. I'm also a person living in long-term recovery from substance use disorders.

MS. SHERIDAN: I'm Kristina Sheridan, and I'm here as an expert caregiver for four children who've got complex chronic conditions spanning infectious disease, autoimmune and dysautonomia. I'm also a researcher and advocate for patient engagement to improve patient self-management and provide the patient voice in these settings and others.

DR. PARKER: Monica Parker, a primary care clinician and Director of Minority Engagement for the Goizueta Alzheimer's Disease Research Center. My work involves educating the community and professional community about opportunities to participate in clinical research and the importance of same.

MS. SCHRANDT: Good morning. Suz Schrandt. I am a long-term patient with rheumatoid arthritis, the type that affects children, JIA. I'm formerly with the Arthritis Foundation and now with ExPPect, a small patient engagement initiative, and serving as a patient engagement advisor to SIDM, the Society to Improve Diagnosis in Medicine. And I should mention I'm the happy recipient of multiple implants that are functioning quite well these days.

MS. LEONG: This is the implant section. Good morning. This is Amye Leong from Santa Barbara, California. I am a patient advocate, really not by choice but by happenstance called rheumatoid arthritis, osteoporosis, thin bones as an Asian individual, and realize that people thought that my ability to speak and translate complicated research data could be very helpful to them. Thus I became a patient advocate, motivational speaker. I have served for 12 years as the international spokesperson for a United Nations initiative called the Bone and Joint Decade and serve at the international level on a variety of different international projects. Patient

engagement is a very near and dear part of my existence because so much about what we, as patients -- and I'm the holder of some 22 joint replacements and other devices in this little body -- that choice is always a factor as it relates to education and information, and certainly our constituency, our public, our citizens, and people who live in the United States have a right to know the kinds of information they need to make the appropriate choices. So I'm delighted to be here.

DR. BHATTACHARYA: Good morning, I'm Dr. Mondira Bhattacharya. I'm an infectious disease physician and have been in industry for about 17 years, currently at MyoKardia in San Francisco. I have been involved in a number of those countries -- companies that I've worked in, in terms of developing benefit-risk strategies and, most importantly, how to incorporate patient perspectives into those strategies.

MR. CONWAY: Thank you very much. And to the public that's watching and listening, I hope you have a sense of the breadth of the expertise and the depth of the patient experience represented here at the table.

We'll now hear remarks from Dr. Ned Sharpless, Acting Commissioner of FDA. I'd like to remind the public observers at this meeting that while this meeting is open for public observation, public attendees may not participate except at the specific request of the Committee Chair.

Dr. Sharpless, you may now begin your remarks.

DR. SHARPLESS: Thank you. I'd like to try and talk to everyone, so I might come over here and --

UNIDENTIFIED SPEAKER: It's not working.

DR. SHARPLESS: From here, if it's okay. Is this a good spot to stand and --

UNIDENTIFIED SPEAKER: That's not working.

DR. SHARPLESS: Sorry. This is not -- it's working now, okay. Good, because I'm

going to need that.

Good morning, everyone. For those of you in the room and watching online, I want to thank you for joining us for the Patient Engagement Advisory Committee, or PEAC, hosted by FDA's Center for Devices and Radiological Health. The Patient Engagement Advisory Committee is a critical tool the FDA uses to bring together patients, advocacy groups, experts, and others to increase patient input into our regulatory process. Hearing the patient voice in these decisions we have to make is very critical to the FDA. And this drives a more patient-centric medical device sort of milieu for innovation, development, evaluation, and access.

Today's meeting also brings together a number of other key stakeholders. We have caregivers and device developers and advocates and researchers and health providers. But the very name of this meeting, the Patient Engagement Advisory Committee, reaffirms just how central patients are to this process.

We take this approach for two main reasons: First, the work we do directly impacts the health and lives of patients; and second, because we understand that today, more than ever, what patients know can and should inform the work we do in a central and very positive way. We increasingly understand that those living with a chronic disease are experts in understanding the effects of a disease and its treatments and, therefore, we naturally seek their input and their voice. It's smart science, and it's good sense to do this.

On both a personal and professional level as a cancer researcher and a cancer doctor who treated patients for many years, I learned just how critical it is to listen to patients when determining the treatment most appropriate for their individual needs. I've seen how increasingly in the era of modern clinical research, we have to gather the necessary data by learning from every patient. In fact, this was sort of my tagline when I was at the National Cancer Institute, you know, that efficiency that you get from learning from every patient,

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

but that requires data collection from every patient.

Today's meeting is focused on a particular aspect of our work, to protect the health of patients, to ensure the safety and security of lifesaving medical devices. When we think about medical devices we use, they ought to be safe and effective. I think that's obvious. But we don't always think that safe and effective includes that they need to be cyber safe. This is sort of a new and emerging problem in devices and, frankly, a very interesting problem but also a very significant problem that we need to address. But, today, with so many of our medical devices connected to the internet and hospital networks and other medical devices, this is an increasingly important consideration.

Whilst interconnectedness offers many benefits, undoubtedly, to personal health, it also increases the vulnerability of these devices to cybersecurity threats. And this risk is increased because many older devices were not built with cybersecurity in mind and use dated software and hardware and protocols. So whether it's a ransomware attack that interrupts a hospital's operations or the exploitation of a vulnerability that compromises a specific device, we face a higher level of risk to the safety and effectiveness of a range of medical devices and to the health of the patients who use them. As patients, you should feel reassured that your devices are safe and effective and not have to worry that they can be hacked or compromised through an attack, through a cyber attack.

As medical devices are becoming increasingly vulnerable to cyber attacks, the FDA has been working aggressively with medical device developers and manufacturers, with healthcare facilities and other government agencies like the Department of Homeland Security, to minimize and mitigate these risks to these devices.

Let me give you a brief example. Imagine that about 5 years ago a family member had a cardiac device, like a pacemaker, implanted to help keep their heart rhythm normal and help in many cases to keep them alive. Recently, patients were notified by the device

manufacturer that an unspecified cybersecurity threat could interfere with the proper functioning of their device. That would be, I would think, as a patient, mildly terrifying to hear such a statement.

To eliminate that threat, the company plans to send an update to the device at home. On the surface that sounds helpful and necessary, except you have sort of no way of knowing whether this fix will work, and there's been a lot of media coverage about the potential danger which is only increasing your concern, and you don't know where to turn for reliable information about the likelihood and probability of something bad happening, nor do you know the potential cybersecurity danger or the risk that might accompany an update to your device. You reach out to your healthcare providers, and they are equally mystified, but it turns out they have a lot of the same questions as there is little available evidence or data to support or inform her recommendation, for example.

Part of our job, the FDA's job, is to address those situations, and we need your assistance. Your contributions and experience can add tremendous value to our efforts to improve the cybersecurity of medical devices. We want to hear from you and understand your perspectives in these areas. We want to learn what we can do to provide you with the information you and your physician need to make those informed healthcare decisions.

At FDA, we recognize the complex environment that medical devices operate in, whether at the bedside or in a patient's home, an ambulatory care setting, a doctor's office, a hospital ICU, an OR, or a radiology or lab facility. In each case, any threat to device security can be life threatening, and that's why we take them very seriously.

Over the past 6 years we've taken significant steps to build a stronger, healthy, and resilient cybersecurity ecosystem. As with all the other medical products we regulate, we consider safety issues across the entire product life cycle from sort of cradle to grave of the product to make sure it's safe throughout its use. The FDA has published draft premarket

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



and final postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks and continuous improvement throughout the total product life cycle.

Of course, the FDA cannot do this alone. That's why a key part of our work is through these partnerships that we've built across government and with industry, security researchers, and patients and providers. Each of these collaborations plays a critical role. For instance, the FDA encourages medical device manufacturers to address cybersecurity risks through monitoring, identifying, and addressing cybersecurity vulnerabilities in the devices after they are on the market. We've also provided incentives for companies to adjust to their marketing and distribution of some medical devices to reduce risk. We've also built strategic alliances with information sharing and analysis and organization of other healthcare organizations. For example, we work collaboratively with the Medical Device Innovation Consortium, which is engaged in a number of projects that explore the science of patient input and cybersecurity.

And we're working to strengthen cybersecurity across the government. For instance, through a memorandum of agreement between the FDA and the Department of Homeland Security, we have implemented a new framework for enhanced coordination and information sharing about potential or confirmed medical device cybersecurity vulnerabilities and threats.

We believe the best teams approach can lead to more timely and effective responses to potential threats to patient safety and to provide for the public health, all of which serves to underscore the importance of today's meeting. At our cybersecurity workshop earlier this year, we heard perspectives from many patients and caregivers related to medical device cybersecurity. Among the important things we learned were that we needed additional conversations to better understand how to communicate to patients

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

about these challenging topics. So today's discussion will focus exclusively on patient perspective and how to talk about the medical device cybersecurity challenge.

To be sure, communicating about cybersecurity threats poses a unique challenge. There are intrinsic limitations in understanding these very complex technologies combined with the uncertainties associated with the devices and how easy it is to exploit the vulnerability of certain devices, and the danger of leaving a single device in a vulnerable state unfortunately can expose multiple devices across systems because of the interconnected nature of things we use today.

So as we increasingly focus on these challenges, we're turning to you for your input and ability to help shape this area and save lives. We want to know what's important to you, what you think is important for patients to better understand so they can take appropriate action in response to our cybersecurity safety messages. We want to hear about perceived barriers and challenges and about the experiences you, as advocates, have had in order to ensure that hard-to-reach populations, such as those living with limited internet access, receive the communications they need on these topics.

I look forward to continuing to partner with patients and advocates to advance FDA's mission and achieve CDRH's vision for all patients to have access to high-quality, safe, and effective medical devices.

Thank you again for your participation today. I look forward to the discussion and comments that come out of this Advisory Committee meeting. Thank you for allowing me to speak this morning.

(Applause.)

MR. CONWAY: Thank you, Dr. Sharpless. We appreciate you being here this morning, and I think it sends us a very strong signal of how FDA has prioritized this issue internally within the senior ranks and through your leadership. Thank you very much.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

We'll now hear updates on the Patient Science and Engagement Program from Dr. Michelle Tarver, a longtime patient advocate, Director of Patient Science and Engagement at the FDA. She'll also provide us with some insights on the impact that this Committee has had over the past several years.

Dr. Tarver, you can begin your remarks whenever it's convenient for you.

DR. TARVER: Good morning. Welcome, everyone, to our Patient Engagement Advisory Committee meeting. Thank you, Mr. Chairman. Welcome, our distinguished Advisory Committee members, our speakers, our audience, those viewing in person and on the web.

So you've heard how important this Advisory Committee meeting is and how it's a central part of the work that we're doing at CDRH. I wanted to give you a little appetizer before we get to the meat of the meeting, which is cybersecurity and how we can better communicate the threats from cybersecurity to patients and the public. But, first, I'd like to give you an update about our program.

The CDRH Patient Science and Engagement Program is inspired by patients and driven by science, and our undergirding principle is to make sure that we not only just hear the patient's voice but that we understand it and incorporate it into all of our regulatory activities as appropriate. And in order to do this, you need people, and so I'm delighted to share with you today that we have a number of new team members that are helping us in this endeavor.

Allen Chen, who's been standing at the door -- do you want to raise your hand, Allen -- is our program manager. He's helping to manage our research portfolio so we can advance the science of patient input as well as tracking the progress of the program.

We have a psychometrician, Fraser Bocell, who I believe is sitting behind me, and Fraser is one of our experts in the analysis and development of patient-reported outcome

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

measures.

We have a psychometrician, Dave Gebben, and he is over on the side, and Dave is a unique person. Actually, at CDRH and at the Agency, quite frankly, we don't have a lot of health preference experts, and he is an expert in how you look at health preferences in the regulatory context.

So we have a number of engagement activities that we have also developed, and you heard a little bit about one of them at our last Advisory Committee meeting where we introduced you to the Patient and Caregiver Connection. This whole program was designed to ensure that our staff have access to timely input from patients about what it's like to live with their condition, interface with medical devices, and what are the concerns that are more pressing in their patient community.

Last year we launched it, and today I'm delighted to say that we have 14 organizations in this pilot program. We introduced these organizations to our staff as part of our CDRH town hall in June of 2018 -- 2019. Excuse me, I'm losing track of time. So at that meeting, we had our staff actually hear not only about the patient organization and the condition but also had the opportunity to hear about all of the exciting work the organizations were doing in terms of research, registry efforts, social media connections in support of patients who are living with their conditions. And our staff saw new opportunities in which they could collaborate with patient groups and get input that's relevant to their review work.

We have sent a survey to all of our members, and we're eagerly awaiting, kind of, feedback from them about what they thought about our questions, what they thought about our program, and what ways they can help our efforts.

So far, my last portion of the updates, I wanted to give you some insight into what we've done from the recommendations this Advisory Committee has provided to us.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Last year, as you heard from Mr. Conway, we discussed patient-generated health data, and by that we meant digital health technology such as sensors, social media, and patient-driven registries. From that work, we heard loud and clear from our Committee that it's important that data is openly available so that patients can be empowered to help manage their own conditions as well as be sentinel surveyors of safety signals.

And so we heard that and generated a letter of support that we shared with the community. That letter of support talks about the principles of openly sharing data that's collected by medical devices. It also helps to encourage the empowerment of patients so that they can be active in the management of their conditions as well as helping to monitor devices that are managing their condition. And we also hope that it will help enrich the understanding of the benefits and risks associated with technology.

At our inaugural meeting, we talked about the involvement of patients in the design and conduct of clinical trials and based on the recommendations from that meeting, where we were encouraged to put forth a framework to help explain ways in which patients can be involved in the design of clinical trials and demystify that process, so we committed this year to publish a guidance, a draft guidance, about patient engagement in medical device clinical investigations. So stay tuned, keep your eyes peeled; we'd love to hear your comments when that guidance document actually posts. But we really do take the work that you all do and the recommendations that you provide to us seriously and want to make sure that we empower patients in the process.

So thank you very much.

(Applause.)

MR. CONWAY: Thank you, Dr. Tarver.

We'll now hear an FDA presentation on CDRH's cybersecurity work.

DR. CARMODY: Good morning and welcome. My name is Seth Carmody, and I am

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

the cybersecurity program manager at CDRH, the Center for Devices and Radiological Health. On behalf of the Center's cybersecurity team, thank you for being with us today and sharing your time and ideas towards solving some complex issues. Today I'm going to provide a brief 10-minute overview of some key concepts and CDRH activities that form the basis of what we'll be discussing throughout the day.

There are many types of technologies that are used within healthcare, and not all of them are considered medical devices. The definition of medical devices can be found in the Food, Drug, and Cosmetic Act. Section 201(h) of the Act -- emphasis is mine -- defines a device as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease or intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action.

For technology that meets this device definition, CDRH's job is to make sure that devices provide reasonable assurance of safety and effectiveness before and after a device reaches the market.

Medical device cybersecurity is defined as the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient. Why do we need medical device cybersecurity? Without adequate cybersecurity, connectable software devices may not provide a reasonable assurance of safety or effectiveness.

Let's continue with some key cybersecurity terms. These terms include asset, threat, vulnerability, and risk. Asset means the things that we care about, the things that are worthy of protection. Threat means the thing that can harm that asset. Vulnerability is any

weakness that can be exploited by a threat. And risk is the potential for harm. Risk is typically an evaluation of the likelihood of an event occurring and the severity of harm if that event occurs. In cybersecurity, the likelihood depends on the actions of a threat against an asset.

Providing probabilistic estimates of a threat exploiting a vulnerability is unknowable, and therefore in cybersecurity, basing actions on probabilities is a trap. As a consequence, tools that FDA uses to assess risk and make benefit-risk determinations can break down. One can perfectly reason why something won't happen and also be perfectly wrong. This is why cybersecurity requires leveraging the concept of exploitability, not likelihood. Exploitability is the feasibility, in non-probabilistic terms, of a threat taking advantage of a vulnerability.

Cybersecurity is a national security issue, and today, the healthcare and public health critical infrastructure sector represents a significantly large attack surface. Devices have capitalized on technological advances, in part by becoming increasingly interconnected. And connecting hearts and bodies to the internet has increased positive health outcomes.

The software that enables these incredible technologies is, like all technologies, vulnerable to threats. And when vulnerabilities are not addressed and remediated, they can be exploited, which can result in patient harm and serve as access points into healthcare delivery organization networks.

While we aren't aware of any reports of patient harm caused directly by a cybersecurity incident, some of the most notable exploits, WannaCry ransomware and the NotPetya attacks in 2017, caused disruption to healthcare delivery by impacting computer systems of the United Kingdom's National Health System and the medical product supply chain. These breaches can compromise confidentiality, integrity, and availability of

lifesaving technology. Specific examples of these types of harms are the release of patient health information, the changing of device settings, and rendering the device inoperable. This is why it is critically important to be proactive in finding and fixing vulnerabilities before exploitation.

FDA/CDRH has been extremely active in this space since 2013. I'll highlight a few key examples including, by the conclusion of this meeting today, five public workshops: one in 2014, '16, '17, and two in 2019. We've published numerous safety communications on the security of devices to help inform the public, patients, and clinicians on appropriate actions to secure devices, and as depicted on this slide, we published two key guidance documents that form a total product lifecycle approach to cybersecurity.

Following an Executive Order and Presidential Policy Directive in 2013 which created a mandate for stakeholders to improve security for critical infrastructure, we finalized our first premarket cybersecurity policy in 2014 entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." It was the first time CDRH provided expectations for medical device cybersecurity design and what was expected in submissions when devices were submitted for premarket review.

In 2016 we finalized our postmarket policy entitled, "Postmarket Management of Cybersecurity in Medical Devices," which set expectations and incentives for managing cybersecurity risk once devices were on the market. Because cybersecurity is an evolving topic, we released in draft in October of 2018, a significant update to the 2014 premarket guidance. We are currently revising that document based on public comment and hope to have an update by the end of the calendar year. These two documents form the basis of our total product lifecycle approach from conception to obsolescence.

The postmarket guidance outlines expectations on addressing cybersecurity risk once devices are on the market. Once issues are found, it is critical to communicate to



those affected by the issues and risk-reducing actions. Communicating actionable cybersecurity information requires close coordination amongst many different stakeholders. In this slide I'll focus on seven key stakeholders: FDA, Department of Homeland Security or DHS, security researchers, medical device manufacturers, healthcare delivery organizations or HDOs, clinicians, and patients.

Each stakeholder has a role to play in the success of cybersecurity communications. For example, a researcher can find vulnerabilities in devices and can provide that information to the FDA, DHS, or MDMs. FDA, DHS, and MDMs work to assess the validity of the vulnerability and the scope of impact if that vulnerability were exploited. And when coordinated well, the FDA, DHS, and the MDM communicate to complementary audiences about the issue and actions that can be taken to reduce the risk. The audiences are HDOs, clinicians, and patients. HDOs, clinicians, and patients are responsible to make sure that the described actions are taken.

To deliver on the promise that technology brings to patients, we need all stakeholders to do their part, and FDA is the principal regulatory body for medical device manufacturers. But while together we've made tremendous strides in medical device cybersecurity, we need help from stakeholders within the chain of care delivery, up- and downstream. While devices may be reasonably secure when shipped to customers, over time they will need to be updated and patched. Therefore, we need the chain to deliver these updates and patches to patients. We need hospitals to patch devices, and we need clinicians and patients to understand the value of applying them. By fulfilling these shared responsibilities, our healthcare and public health critical infrastructure will change from brittle to resilient.

Thank you.

MR. CONWAY: Thank you very much.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

(Applause.)

MR. CONWAY: We'll now hear a presentation from the University of Michigan concerning cybersecurity and medical device updates.

DR. FU: Hi, good morning. I'm Kevin Fu, a professor at the University of Michigan in electrical engineering and computer science. I don't have any medical devices, but I do have a cold today.

Let's see, moving forward. Let's see. The next slide, please. Okay, there we go. I see. There are my disclosures.

A lot of thank-yous. I'm going to represent some comments from a number of different organizations having to do with medical device safety and computer security.

And just a little bit about my background. I did grow up in healthcare IT, working in a small community hospital back when we were trying to roll out paperless medical records in the early 1990s. But these days I'm a professor working in computer security and how it intertwines with physics and the delivery of healthcare.

So I'm going to argue that the correctness of a medical device or any kind of computer is relatively easy compared to security, so I usually quiz my undergraduates, how do you define the security of a little key entry pad into a building, and the students usually say, well, if you enter the passcode, the door should open. And that's a relatively reasonable definition. But if you ask how to define security, it's a lot harder because, like safety, it's a negative goal.

So in the case of this particular hotel, they actually printed a plastic placard with the PIN code, and they also have the PIN code in Spanish if you can't read the English numbers. And why did this happen? Most likely it had to do with miscommunication about the specification and, you know, interesting design maybe by committee. I don't know.

But moving forward, computer security is hard to get right in general. Getting it

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

right with medical devices is even harder. But there are significant benefits, for instance, to computing and wireless technology. One of the earliest devices for cardiac patients was a pacemaker, but it had no wireless communication. Instead, it had the little needle that you would have to plunge through the patient's skin to twist a small dial in order to change the pacing rate. This introduces obvious risks of infection, and so having the wireless control significantly reduced those risks.

However, of course, there can be new risks, and those new risks in this age happens to be computer security. So in my own work, I've been working in the security of pacemakers and defibrillators and other medical devices for around about -- let's see, let me do the math, about 13 years now, beginning in 2006 visiting FDA. And our most notable work was showing how to reverse engineer the wireless control of a pacemaker and defibrillator in 2008.

Let me just highlight some of that work from 10 years ago because it's still relevant today, especially with some of the advisories that have gone out in the last year from the FDA.

So typically with an implant, you will have the healthcare team set information about the patient on the implant wirelessly, using some kind of radio communication. It's surgically implanted, and then there's a test to make sure, for instance, if it's a defibrillator, that it's working properly. And then the patient is usually given some kind of device they take home for some kind of continuous monitoring so that if something should go awry, the clinical team can get an early warning on that.

So 10 years ago, a group of my students took a look at what was the radio communication going between the implant and this programmer that the clinicians would use in the clinic, and they discovered that it was not encrypted and they could derive all of the patient information, the name, the device state, date of birth, all that kind of

information, effectively an electronic health record just being broadcast to anyone who could create a receiver. And these were graduate students who had never worked with medical devices before.

But more surprising to us was that we were able to induce the conditions necessary for a fatal heart rhythm. So the students built, effectively, a tape recorder that would record the radio communication and then replay it back. So they recorded the command to disable all the therapies, and then they also recorded the command to induce what's called the command shock, which to an electrophysiologist means sending a pulse to the T-wave that would cause this chaotic heart rhythm and the patient would go into what's known as V-fib. No amplification was necessary, and this was a proof of concept. We couldn't find any volunteers to engage in this, so instead we tested a small resistor and were able to show that it did indeed cause this effect.

But where are we today? That was 10 years ago. We are still seeing it takes 10 years to fix some of these problems. Today the problems are just getting harder. We're seeing ransomware. We've already heard talks from Seth on that. This is a screen you may see from time to time. I'm sorry if you clicked on the button that caused the ransomware to install on your computer, but it happens to the best of us. I know many computer scientists who have been infected by ransomware. It encrypts your hard drive and prevents you from getting access to your information until you pay a ransom or until you restore from a backup.

But like most things in the U.S. government, we should turn to the Russians, and the Russians have actually figured out what might be the most effective way to solve ransomware; they spritz holy water on their computer systems. And this is only a half joke, and the reason why I call it a half joke is if you think about it for a moment, all the technicians sitting around these computers in Russia, they're more aware of the computer

security risk and they're probably doing better hygiene at this very moment. Even though it makes no sense to spritz water on the computer, they're probably thinking about it. And I ask you today, how often do you think twice before inserting a USB drive a second time in your computer and how often do you use a syringe twice? So think twice.

How do we move forward? Security really needs to be designed in from the beginning of the medical devices, not at the testing stage but at the whiteboard stage, very early in the development and the manufacture of medical devices, not bolted on after the fact. In fact, I have this child booster seat, and it was recalled by the FDA some years ago, not because of the duct tape.

There are also a number of engineering guidance documents. This is not an engineering meeting, so I won't go into great detail, but there are a number of standards documents that the FDA recognizes, which I believe is pushing forward the safety and security of medical devices at the very early stage.

And I also want to hone in on another topic Seth had mentioned just a few moments ago, and that is how likelihood is a trap. I think we're quoting Billy Rios, among others, who tried to explain that using probability to reason about security, you know, your heart is in the right place, but it's misguided, and the reason why is in safety we like to think about normal distributions, mother nature, Gaussian distributions of failures, so the past tends to predict the future. But with computer security, you're dealing with an adversary who is intentional and is malicious, and if there's a 1% chance of a failure, that adversary will make that 1% one hundred percent of the time. These are typically through the black swan events, so it's very dangerous to use the past to predict the future. You're really dealing with the Three Stooges there.

A few words of caution about how to move forward: There's a lot of blaming that goes back and forth between various stakeholders. I would just say be careful of blaming

various vendors, manufacturers, and healthcare delivery organizations.

A lot of folks will ask me, like, is my medical device secure? I would say more meaningful questions you can ask than these sort of yes/no would be how gracefully can a medical device tolerate a computer security threat? It should not go into a catastrophic failure mode, but it may go down into some kind of degraded mode that needs attention later.

What kind of controls can we put in place to reduce these risks even if the device is hacked? So just like there's no crash-proof car, there is no secure, ultimately secure, medical device. But we can reduce the risk to keep it safe enough.

I would say with cybersecurity we always need to think with patients first. The biggest risk, to me, is not hackers breaking into medical devices; that is a real risk, but the biggest risk, to me, is the wide-scale unavailability of patient care, entire hospitals going down. That's why ransomware is such a big issue. But also the integrity of medical sensors, because we are finding many medical devices today are becoming closed-loop systems, for instance, the artificial pancreas, and if the sensor is compromised and causes the computer to make an automated incorrect decision at population scale, that could be catastrophic.

There are a number of gaps. I won't go into the details today, but I'd say the main challenge, at least in the clinic, is not interrupting the workflow. We all hate entering passwords on computers. It's even worse inside a hospital when you're inside a sterile field and you're wearing latex gloves. Don't interrupt the clinical workflow if you're a security practitioner. Many security specialists in the healthcare industry are very good at what they do, and they tend to focus on technical controls, and many safety specialists tend to focus on risk management. I would say we need both of these kinds of schools of thought in order to push the needle.

I'll end there, but I'd be happy to take questions later or after the event. Thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MR. CONWAY: Great, thank you very much.

(Applause.)

MR. CONWAY: We'll now hear a presentation from the University of California, San Diego, concerning physician perspectives on cybersecurity.

DR. DAMEFF: Excellent. Can everyone hear me all right? It's a true honor to present here today. Thank you for the invitation, and thank you for the service that you do for your country and the patients of this country.

My name is Dr. Christian Dameff. I'm an Assistant Professor of Emergency Medicine and Biomedical Informatics at the University of California, San Diego. I also am a security researcher looking at the intersections of patient safety and cybersecurity in a variety of different domains, medical devices, critical hospital infrastructure, etc. I have no relevant disclosures.

And I'm here to talk about what I think is a near and dear topic to myself in really an evolving space really at patient safety, patient education and awareness, as well as physician education and awareness, and that is the topic of informed consent. Now, informed consent is not a new concept. It is definitely not something that is practiced ideally across the country, and we'll talk a little bit more about that, but there is some nuance to this now, where we're talking about cybersecurity and informed consent and how that influences the process that doctors and patients have.

Now, when I took a straw poll in preparation for this talk of over two dozen physicians, I asked them what is informed consent, and undoubtedly, every single one of them said, well, it's a form. And then I told them, well, maybe the embodiment of it is a form, but hearken back to the days of medical school when you were taught about ethics. Informed consent is a process. Informed consent is part of the physician-patient relationship, and it is probably one of the most important embodiments of that relationship

because it is the dissemination of information, some of which can be very complicated, all of which involves the health of the patient and their particular outcomes and talking about that with their patient, making sure everyone's okay with that, understanding the risks associated with healthcare. So after I said, well, it's really more of a process, they said, oh, yeah, well, of course, but they talked about how it really -- that the conversation would always devolve into what it is in practice.

And so I'm going to talk about a little bit of a tale of two informed consents, the first of which is a patient, Mr. Reeves, comes into the emergency department at 3:00 a.m. He was cooking. He was cooking at his kitchen and with a knife sustained a laceration to his left hand. This laceration is pretty superficial; a few stitches should work. They work through the initial diagnostics, and the physician comes and recommends some sutures to the patient. The informed consent process then begins and after a few sentences quickly discussing risks of infection, risks of nerve damage, etc., the consent is done, and both the patient and the physician feel comfortable about the risks of a procedure, namely, a few sutures. And that's perhaps embodied or recorded in a document that is half a page to a page long.

Let's contrast that with another tale. In 1999 Sir Elton John had a pacemaker placed. I'm going to completely speculate as to the level of informed consent detail that happened during that, but I imagine it was quite extensive, perhaps dozens of pages. Half an hour to an hour of conversation alone regarding the risks of anesthesia, the risk of the pacemaker itself, complications of infection, etc., and that probably involved not just the patient and the doctor but probably other parties and representatives around Sir Elton John to come to the ultimate conclusion that this piece of implantable technology would benefit the patient.

Now, these are two patients, both with the same rights, both undergoing medical procedures that have vastly different informed consent processes. The question I would



pose to this Committee and to this body here is what do we want cyber informed consent to look like? Do we want it to look like a line on the boilerplate of a form, 16 items down, that's never talked about? Or do we want cyber informed consent to be a 30-minute discussion every single time a patient gets a pacemaker or another implantable connected medical device? I would pose that there is really no right answer, but these are the questions we're going to struggle with because, in practice, the doctors are mostly in charge of this, and whether or not the doctors raise this question even to the patient is an unknown.

We'll go over some quick elements of informed consent because they are so key to the patient perspective. First, in informed consent, we identify the right patient. There had been problems with that. We talk about the purpose of the procedure itself, the benefits. If you get this procedure, this is what will happen. If you don't get this, this is what might happen.

The risks associated, and again, we're going to talk more about this. This is so key. When I am talking to a patient about the risks of a blood transfusion, I can quote them the past and say you have one in, for example, 100,000 or a million times of a blood transfusion to get HIV, because I have data to show them those risks or I have experience from my past patients to be able to talk to them about risk in a meaningful way. That's what patients want. They want to understand what is the probability of something happening. We talk about the alternatives to treatments, we answer their questions, and we want to make sure we get affirmation from the patient if they want this. These are all parts of informed consent.

Now, true informed consent is a two-way process. I asked my physician colleagues the same question, well, how do you know when informed consent is done? They say the form is signed and I can get on with the work. And I say, well, that's not really the case.

Were you paying attention in medical school? Perhaps you should go back to that ethics course. No, it's really an ongoing process and an evolving thing as things change, but also it's a two-way street. Not only does the patient have to understand the document and sign it, but the physician should understand the document. That's really key. If the physician or the clinician, whoever's engaging in this patient communication, does not understand the elements of informed consent, then maybe they're giving the patient the wrong information.

Now let's talk about the challenges of cyber informed consent. Again, we can get through most of these until we hit risk, and I'm really glad this has been talked about at least twice before.

When a patient asks me, if a patient should ask me what's the chance that I'm going to get hacked, I can't look them in the eye and tell them the risk, I don't know. I don't think anyone knows. I think anyone who purports to say they know doesn't really. And that's also something that can change dramatically. We often say we don't know about a patient who has been adversely impacted by cyber harms, but that could change overnight, and that could change and not just be one patient, it could be thousands of patients, perhaps, overnight because it does not fit the traditional risk curve. Exactly as mentioned previously, the past will not predict the future in this. And traditional technologies that we thought might be safe or haven't had reports of any issues for years and years and years can then, in the future, become huge areas of cyber risk concern. So in this cyber informed consent process, when a patient asks me what's the risk, we don't know. That's not very confidence building with our patients.

Next, there's alternatives as a key part of informed consent. In certain device categories there might not be alternatives that are connected, especially as we move forward and understand the benefits of connected medical technology. The device that you

get implanted in you is often not your choice. It's often physician preference, what they trained with, for example, what's available to their particular hospital, what they've negotiated with insurance to be covered, etc. So there may be a situation in the future where a patient can't even choose a device that's not connected. That's really an unfortunate and kind of scary prospect, that if you want to get this medical technology benefit, you have to be connected. That's something I think we should really dive into.

Another really important part of cyber informed consent is going to be this process of questions. Now, I took another informal straw poll of over two dozen physicians at my facility and asked them what cybersecurity was, and they said it was hackers stealing my banking credentials, etc. I said what about cybersecurity in healthcare, and they said, oh, I heard something about ransomware attacks.

This is a huge problem, and something that really frightens us in this space is that we can do all of this great work to educate patients, even medical device manufacturers to continue to design better and more secure medical devices, but at the end of the day, if we don't spend time educating clinicians, then they won't understand it and they won't be able to answer patient questions.

Now, this is a tall order in healthcare, generally, where you do educate doctors about the latest and greatest prescription drugs or treatments. It's hard to just educate them on the important medical things. Now we have to add into their docket being educated on the issues of cyber, and that's a really hard thing to do. How do you disseminate that information to thousands and thousands of clinicians in real time on a very complicated topic that they quite frankly have no expertise in, generally?

Now, despite all of these daunting concerns I have about cyber informed consent, I really decided to let go and say we should embrace it wholeheartedly because it's opportunity to provide tremendous benefit in this space. It might be unparalleled. This

might actually be the secret sauce intervention, if you will. Let's talk about that. First of all, it's just the patient's right, and it empowers them, and it's what they deserve. They should be able to get an implanted medical device or just interactive medical technology that's connected and have their question answered about cybersecurity risks. That should be a non-starter; they deserve it.

But two is an opportunity for patient education. The other side of this coin is if patients are educated by news headlines that are shocking, then it could deter them from engaging in healthcare; it could deter them from getting that lifesaving medical technology. If we allow for this to be the real point of patient education, to provide them the most accurate information in a doctor-patient relationship, that's going to be key. So cyber informed consent will allow for increases in patient education on the topic.

The third point here: As I mentioned in the previous slide, we're very concerned about educating physicians and clinicians about this. This document may force them into that, right? If it's the fourth line or fifth line on their informed consent document that they're going to do two dozen times that day in the OR, they're going to ask questions about it, and in that opportunity, we can educate them. If we provide them accurate resources and education in this, we may be able to have that educational opportunity because informed consent is required by every hospital performing procedures.

It's going to raise awareness and possible detection of adverse events across healthcare, so this is really key. So I also get asked, show me someone who's died, show me someone who's been harmed, and my response to that question is we lack the telemetry, we lack the sophistication to likely detect these adverse events. This isn't disease registries. We don't have a test for cyber, that way I can take some blood and see if you've been hacked. We don't have processes in place to even pick up on this. So my thoughts are if we build in cyber informed consent into this process, the increased awareness will then allow

us to detect, with better accuracy and sensitivity, possible adverse events related to this.

And then, lastly, it's just an important thing. It may bridge the gap early between the devices themselves, the clinicians, and the patients. It's kind of the glue of education between them.

And that's what I wanted to spend my time here talking to you about is this issue of cyber informed consent. If I have any time, I can take questions from the panel.

MR. CONWAY: Great, thank you. We're going to hold questions until we do our open public discussion, but thank you very much.

(Applause.)

MR. CONWAY: We'll now hear a presentation from Thermo Fischer Scientific concerning cybersecurity vulnerabilities.

MR. RADCLIFFE: Thank you. I'm really excited to be here speaking to you today. I spend most of my time talking to computer people. I am somebody who works in the computer security field, or as my kids like to call me, I'm a good guy hacker. And I've been doing this kind of work pretty much my entire life. My dad loves to tell a story about how when I was three, I figured out how a screwdriver worked and I took apart every doorknob in my house because I wanted to figure out exactly how it worked, and he says I've been doing that pretty much with everything ever since.

One of the things that was very interesting in my life was at the age of 22, my 22nd birthday, I was diagnosed fortunately with Type 1 diabetes. I say fortunately because it gave me something new to tinker on; it gave me something new to look at. I was somebody in the computer security field. I had a lot of background in computer security and in radio communications as a ham radio operator, and I went looking at my device, my Medtronic insulin pump, and I wanted to see what kind of things it could do. Very similar to a doorknob but something that kept me alive.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

So I conducted my own research on my own insulin pump in 2010 and 2011, and I found some really interesting stuff, stuff that I thought was pretty cool. So I put together a proposal to speak at a conference that I thought a couple, a handful of people would come to and kind of see my work in reverse engineering the wireless communication with an insulin pump, and what happened was this huge talk where I had to give a press conference and do all of these things that I was totally unprepared for.

But what I had found was that the wireless communication for my insulin pump was not very well protected. I was able to create a program that turned the insulin pump off remotely. More scary was I was able to change all of the therapy settings remotely as well. This came as a huge shock to not only me but to a lot of people in the world.

And one of the things from the patient perspective that I was unprepared for was the amount of questions that I would get directly to me through email. I had parents emailing me, wondering if their child should be on an insulin pump anymore. I had parents coming to me asking me if they should wrap their kid's pump in aluminum foil, right? I had a lot of questions and concerns from patients like myself about what to do with this information. My insulin pump is hackable. What now? And that's a very scary thing from the perspective of a patient or even a doctor.

Combining this fact, we were very new in this industry and in this world of vulnerable devices, and the company itself, Medtronic, was not fully prepared for that type of disclosure, which made it very hard to communicate that information outwards.

As you can imagine, at the end of the life of my Medtronic pump, I got a new insulin pump, and I bet you can guess what I tried to do with that insulin pump. I got an Animas Ping insulin pump which also had wireless communication. So, yet again, I had a new toy to play with, and I decided to reverse engineer the communication of that device. Lo and behold, I found pretty much the same issue, that the communication between the remote

and the insulin pump was not effectively secured.

It was quite a bit different this time around. The industry had matured much more. I was able to go to Johnson & Johnson with that information, and Johnson & Johnson was prepared. They said, oh, we have a program set up for this, and throughout the course of about 6 months, we worked together on trying to come up with a communication plan for the patients that had these types of devices. And I thought about my experience as a patient and as a researcher the first time around in 2011, especially with emails that I had gotten and communications that I had gotten from caregivers, from parents, and I thought about that, and having children myself, I thought I should probably do more to speak to the patient and less so about the technical details of the wireless vulnerabilities that I had found.

So when we went to disclose this information, I wrote up a blog post specifically for patients, and I said, look, this is a significant thing. It presents a risk. But everything that we do presents risk, and I always talk about this when I talk to people about flying. People take a risk when they fly in planes and something catastrophic can happen. The airplane can fall out of the air and everybody can die. But has that happened a lot? The impact is very high, but the probability is very low.

So we take risks every day when we do these things, and from a patient perspective, I want to communicate, and I communicated in that blog post that I wrote, I said if I had a child that was diagnosed with diabetes and my doctor said to use this insulin pump, I would feel comfortable with my child being on this insulin pump, even with the security vulnerabilities that were found on it. Because I think that when we look at the risks associated with these things, as it sat in 2011 and as it sat in 2016, while the impact could be very high, the probability is very low, so low it's kind of like flying in an airplane. It's extremely safe, and the benefits that you get from using these types of devices far outweigh

any risk that might come from a vulnerability such as the ones that I found. And I think that that's very important.

One thing that is interesting, as I had moved in between these two periods of time and I had a new endocrinologist, I went to my endocrinologist, and he asked what I did for a living in the interview, kind of, and I said, well, I do computer security work for a living. He goes, oh, that's really interesting. He goes, did you hear about this guy who hacked into his own insulin pump in 2011? And I kind of chuckled, and I said I'm familiar with the work.

(Laughter.)

MR. RADCLIFFE: And he went into it, and I said, well, actually, I'm the one that did that research, and he goes, no, you didn't. So we had a talk about it, and when he realized I was the one that did the research, my doctor's appointments became twice as long.

(Laughter.)

MR. RADCLIFFE: While it's interesting and amusing, it's also very important to show a gap here. The first half of my doctor's appointment is me informing my doctor of the current event and the current status of diabetic devices and cybersecurity. While I love this portion of my doctor's appointment, I can't scale -- I can't inform all the endocrinologists of the cybersecurity issues of diabetic devices every 3 months like I do my doctor. That is one of the big challenges that we face right now, is educating the people that are in front of the patient and making sure that they understand and get regular updates on what is going on with the devices that they are prescribing to patients. Those caregivers have a desire for that knowledge and a desire and a need for that knowledge to be explained to them in a way that they can understand it, and that is one of the big things that we need to solve going forward because I can't -- like I said, I can't speak to every endocrinologist that I meet, and I would love to, but it just doesn't scale in that way.

What's interesting as we go forward into the future is the security vulnerabilities

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



that I found have low probability and a high impact. You have to be in the physical space of that person to be able to do anything of consequence. The new devices are not like that. The new devices are tied to your cell phone, and that cell phone is connected to the world. This changes things dramatically when it comes to risk because now we have different pieces of malware that can infect a cell phone that could impact patient care directly. Whether it's a diabetic device, a neurostimulator, a pacemaker, all of these medical devices are using the cell phone as a bridge over Bluetooth. And while there is some security there, no device is perfectly secure.

So we have to be very aware that we have some better things coming, we have more communication coming, but we also have more risk coming. Especially as we move that data to the cloud, doctors have more visibility into their patients' conditions. They can diagnose things faster, more accurately, and better than they ever have before. But now we have all the patient data up in the cloud where maybe it can get accessed by other people. And that's something that we need to keep an eye on.

Is it safer? That's a good question. As researchers, we try and look to make sure those devices are as safe as they can be. As practitioners, we try and make sure those devices are as safe as they can be. And as a patient, I want to know that companies are doing the best that they can to make those devices as safe as they can.

That's all I have for today. Thank you very much for your time.

(Applause.)

MR. CONWAY: Thank you for your candor and your patient insights, very much appreciated.

We'll now hear a presentation from the FDA on CDRH's communication of medical device vulnerabilities and safety concerns.

MS. DUCKHORN: Good morning, my name is Jodi Duckhorn. I'm the Acting Deputy

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Office Director of CDRH's Office of Communication and Education. Today I'm going to provide you with an overview of CDRH's communication process.

Issues that may need communication are identified through a variety of mechanisms. Some of these include:

- Notification from a manufacturer;
- Monitoring of real-world evidence, such as information from registries;
- Social media monitoring;
- Information from post-approval studies;
- Information from complaints or allegations;
- Or a need may be identified by a CDRH employee, such as a safety issue identified during review of a submission.

Once a communication need is identified, a communication specialist leads a team of experts across the Center from a variety of scientific, medical, legal, and regulatory backgrounds to develop consensus on messages for public communications. The communication team also includes a specialist who provides expertise on digital content strategy, web metrics, and stakeholder engagement.

The CDRH communications specialist works with the team to assure messages on public health and regulatory issues are scientifically accurate, consistent with CDRH's mission and goals, and are meaningful to our audiences.

When deciding to communicate, CDRH thinks through the questions listed on this slide. We prepare communications, both internal to the FDA and externally, when there is a need to inform varying audiences, such as healthcare providers, patients, research groups, academia, or manufacturers, about medical device safety issues or innovations, regulatory updates, or Center or Agency initiatives.

After considering the questions listed on the previous slide, CDRH makes a decision

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

about whether or not to communicate. The rationale behind those decisions are included in the next few slides.

CDRH may decide to communicate because communication could minimize any potential risk to device users by altering the way the clinical community or the public use a product. It could help prevent potential or additional harm to device users. It could explain and clarify a complex issue for the public, for example, device use or distribution or a published scientific report.

Communication could expand the reach of a communication previously issued only by a device manufacturer. We may choose to communicate because it would assert FDA's role in an issue that has generated media interest or has been addressed in a professional publication, or if it would help the FDA collect information to better understand a problem. A communication could notify the clinical community of shortages and potential alternatives or increase public trust in the FDA through transparency. It could protect the health of a vulnerable patient population, for example, pediatric or elderly populations. And we could issue a communication to support Agency and departmental goals and initiatives.

There are reasons we may decide a communication is not appropriate. Those might include if the communication could cause unnecessary or disproportionate concern over health risks or cause someone to stop beneficial treatment or stop using an effective device; if the communication could cause someone to perform unnecessary remediation or if it could cause needless anxiety over an implanted device; if it could interfere with a regulatory or a legal action; or if it could contribute to a device shortage. We may decide not to communicate if the communication will not minimize the risk or if it will simply repeat a message that we already disseminated with no added value. We may not issue a communication if the preliminary recommendations contradict established professional

guidelines or professional standards of care or if the preliminary recommendations deviate from the FDA-approved labeling.

Once a communication need is identified, CDRH's communication process begins. The communications specialist proposes a communication to Center leadership, including the rationale for communicating on a specific topic. A working group develops a comprehensive communication strategy and determines the key messages to communicate. The communication plan includes our intended audiences, key messages, and the outreach strategy.

The communication products, such as a safety communication, letter to healthcare provider or stakeholder email, are created using the key messages developed during the communication planning phase. The communication products are then cleared by varying levels of leadership throughout CDRH.

The communications are distributed as identified in the communication planning phase. Dissemination can include distribution through email lists, posting to the FDA's website, tweeting or posting on Facebook.

After distribution, CDRH evaluates the success of the communication through social media monitoring, website hit tracking, Google analytics, and repeat of messaging among other media or others.

CDRH communicates to a variety of audiences including patients, caregivers, healthcare providers, medical device industry, and other stakeholders. When the primary audience for communications is patients and caregivers, CDRH posts information on the [FDA.gov](https://www.fda.gov) website as a Medical Device Safety Communication. The current safety communication template used by CDRH provides a summary of the safety concern, recommendations for patients and caregivers, additional recommendations for healthcare providers, and the FDA's action to resolve the safety concern.

When the primary audience for communications is a healthcare provider or healthcare providers, CDRH posts information on the [FDA.gov](https://www.fda.gov) website as a letter to healthcare providers. Letters to healthcare providers provide details on the safety concern, recommendations for healthcare providers, and detailed information on the FDA's evaluation of the issue and actions to resolve the safety concern.

CDRH faces numerous challenges when communicating safety concerns. These include those outlined on this slide. Health literacy is defined as the degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions. In the U.S., this amounts to 46% or nearly half of the U.S. with limited health literacy. Health literacy affects people's ability to navigate the healthcare system, fill out complex forms, engage in self-care and chronic disease management, and understand concepts such as probability and risk.

Research from the risk communication field suggests that audiences who are emotional or under stress may be less receptive to communications about risk and recommended actions. Stress or emotion may affect how people process a safety communication.

In addition to limited health literacy and cybersecurity understanding, CDRH also faces challenges with communicating to individuals for whom English is not their first language. The 2017 results of the American Community Survey of over 120 million households found over five million households were a limited English-speaking household. Over three million spoke Spanish as their first language with over two million speaking other languages. Additionally, using plain English doesn't necessarily help people who don't speak English as their primary language and who have limited ability to read, write, speak, or understand English. Moreover, simply translating health information into a person's native tongue doesn't guarantee that non-English speakers will be able to read or

understand it.

CDRH, along with most of the federal government, relies heavily on the web and email to distribute communications about safety concerns. The challenge is approximately 10% of U.S. adults do not use the internet. These tend to be some of our most vulnerable populations, including:

- Older adults, particularly over the age of 65;
- Adults with a household income of less than \$30,000;
- Adults with a high school education or less; and
- Adults who live in rural areas.

We also have to consider accessibility for all. More than 13 million people in the United States have at least one disability, and many use assistive technology like screen readers.

When deciding which communication vehicles to use, the FDA has to consider accessibility of the communication for all users. Section 508 of the Rehabilitation Act requires federal agencies to make all electronic content accessible to people with disabilities. If communications are not accessible, it may prevent a member of the public from knowing about or receiving vitally important information.

CDRH uses multiple vehicles or channels for communicating safety messages, which are listed here. In some cases, the CDRH communication specialist works with communications specialists from other areas of FDA. For example, for press releases and media interviews we work with the Office of Media Affairs. And for items like FDA Voices or consumer updates, we work with specialists in the Office of External Affairs.

Here, the help desk refers to CDRH's Division of Industry and Consumer Education in the Office of Communication and Education. They answer questions from consumers, industry, and other stakeholders. Regarding social media, CDRH currently uses LinkedIn,

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Twitter, Flickr, Facebook, and Pinterest. All communication strategies about a safety issue use a combination of these vehicles.

Communication strategies incorporate dissemination of materials through multiple channels used by intended audiences. In addition to posting information on the FDA's website, the primary methods CDRH uses to disseminate information is through email marketing, social media, and targeted outreach to impacted stakeholders. Often the messages included in FDA's communications are redistributed through other channels such as major news outlets, trade media, advocacy groups, and other government agencies.

Now that I have provided a broad overview of CDRH's communication process, I want to briefly delve into specifics about CDRH's communication on cybersecurity safety concerns.

Since 2013 the FDA has released eight unique safety communications related to medical device cybersecurity concerns. As new information became available, the FDA provided this updated information through additional communication. However, communicating about cybersecurity can be difficult.

Cybersecurity has the unique challenge of communicating potential cybersecurity risks for which the probability or likelihood of harm is not known. For most safety messages, the FDA may not know the probability of the device failure, the types of harms, and their associated likelihood of occurring. In most cases, adequate information is not known to quantify the risk because that typically relies on historical data to predict when a vulnerability may be exploited.

It is extremely challenging to understand the motivations of unidentified, unauthorized persons, predict when they may act, identify what vulnerabilities would be exploited, isolate the action to one type or brand of device, and capture the risks associated with that exploitation. In addition, there are challenges and risks in updating devices,

including failure to function, device damage, need for additional surgeries, and potential out-of-pocket costs to the patient.

The lack of cybersecurity risk quantification can impede informed decision making between patients and healthcare providers in determining whether the benefits of a patient receiving device updates for cybersecurity concerns outweighs the potential risks of undergoing the updates. Understanding how unknowable risks are weighed against knowable risks is critical to help address these communication challenges.

Thank you for listening to this overview of CDRH's communication process. I look forward to hearing the conversation and recommendations from today's participants.

MR. CONWAY: Great, thank you very much.

(Applause.)

MR. CONWAY: We will now hear a presentation from the Health Literacy Media concerning cybersecurity vulnerability communication.

DR. O'LEARY: Good morning. I'm Catina O'Leary. I'm the president and CEO at Health Literacy Media. My disclosures are here.

So people have been talking all morning about, really, this slide that I have in front of you now. We're talking about a delicate balance between the benefits of patient care and the risks of security. On the patient care benefit side, we're really thinking about convenience. For many patients, they're living with diseases that they've been struggling to manage on their own for many years, and many of these devices can help make the management of their condition much more easy for them.

In the context of their life, they can provide a more coordinated care for them, where they have access to communication with their providers without them having to facilitate that themselves all the time. It can provide a precision in their care so that they don't have to think about dosing, which can be quite complicated. And it can allow some



prediction. For folks that I know that have devices, this is really life changing. So that side of the equation, that balance is really important. But we have to weigh that against the security risks. So we talked a little bit about patient safety but also the privacy issues. We've not talked a lot about privacy yet. The financial and liability issues and then, of course, the known and unknown risks in an ever-changing and evolving threat environment.

We really think about this in a communications perspective as a tangle of challenges. When we think about health communications, we think on both sides of the communication, the communicator and the audience. And the job of the communicator is to share the information that the audience needs to know, and they need to understand the difference between the need to know and the nice to know and the timing of that.

So in this tangle, we have to think about cybersecurity as a challenge because it's such a complex topic and it's very hard to simplify. People have talked all morning about what we know and what we don't know and the complexity of communicating the unknown in that way.

We also can't often put this risk in numbers. The probability and possibility of the unknown risk, and it's unspecific, is very hard. And then from the health literacy perspective, which Jodi just referenced, the actual numeracy challenges are the most complicated thing that we ask people to do. We're asking them to think about probabilities that are unknown, that are beyond the scope of what people have even learned to do often in math. We're competing against false sources of information and very complex information in that way. And then there's the uncertain timing; we don't know when something will happen and what it will actually be.

From the audience perspective, this concept actually requires incredibly abstract thinking. Again, this unknown risk, people don't understand what it means for them in their space with the device they have right now and how that changes over time. So you really

have to think outside a box that you then can see.

We talked a little about health literacy earlier, but this really overlays with technology literacy, literacy and education. So all of these things are packed together. And also the health literacy factors that were mentioned earlier are important, but the thing that wasn't mentioned is how dynamic health literacy is. So while you might be quite health literate on the device that you first have, as your devices change and your health condition is changing, you add devices. Every single time you add on a layer, your health literacy shifts, and what you know starts again at zero and you have to learn again. So even most educated people can have health literacy challenges as they move through these complex situations.

The concept is new, so there's often no frame of reference, and that's how we learn as people is we structure information on things we know and we expand from our frameworks. So we're asking people to do something that's really outside the scope of their reference.

And then over time we learn about new threats in many fields that are not directly related to our devices, but these messages become scary and then not so scary when nothing happens, and then we hear them again, and this alarm fatigue can make it hard for people to attend to messages and pay attention consistently.

So all of these tangle of challenges are what we're facing, and we have to figure out how to put these all together and make some sense out of them so that people don't have to try to figure that out on their own.

So what we know is people don't think about this all the time. What they do think about is the probability that their device will work and keep them healthy. That's the most important thing for them. They trust the medical professionals that are guiding them, they care about whether the device works, they think about that, but they're not thinking about

all this risk stuff with cybersecurity necessarily. And we know that this is true because we fail to follow cybersecurity best practices in every part of our lives. We're all walking around with phones that probably are begging us for updates that we haven't done. We were sort of joking at the table earlier. My iPhone has an update from about 4 months ago that I refuse to do because I know that when I do it, everything attached to that is going to cause me a problem, and I just don't want to take the time to deal with all the other stuff. And their security update is not really my priority. I don't really care about the little miniscule risk that I don't understand, and it doesn't matter until it matters.

And a majority of Americans really expect something to happen. They just don't know what it's going to mean to them, and they haven't had an example of how big this risk could be and what sort of magnitude of the exposure could be. We're not thinking yet about the probability of a compromise and the magnitude of harm. And we're also not really thinking about the value of our personal health information and how identifiable that is and what it means to be on our device.

So, again, I mentioned a little bit about alarm fatigue just a second ago, but the other piece of this is cognitive overload. So we think about the amount of work that is associated with all these things that we have to do. There are frequent alarms. This causes people to want to stop using systems because they feel sort of uncertain and they have to think about what this means, how much it's a problem, whether it's complex, and then they have to distinguish is this important information or is this unimportant, does this matter to me or does it matter now, and they get repeated exposure over time so they just stop paying attention. So the number of notifications that pop up and tell us to do something that are not meaningful really shifts what we think is important.

So from a stakeholder perspective, there are a lot folks involved. I think the earlier slide that someone showed identified seven or eight different stakeholders. I sort of boiled

that down to three. There are the people who are sometimes patients and sometimes are not. So this is another story of health literacy. We're always people living our lives, and sometimes we focus on our health, and sometimes we're patients. The rest of the time we're doing other things and living. There are also healthcare providers and organizations who are involved in this and then inventors and manufacturers who are very involved. And then I list the FDA, but we think about government more broadly than that as people who are involved.

So what we agree about, all of these groups, but we use different words, is safety, right? First and foremost, safety, and we mean that in a very broad way, including security, cybersecurity, all of these things. We don't agree on a lot of other things, including what's an acceptable risk and at what cost can we reduce those.

But in each of these areas there are opportunities to communicate. So if we think about between the people who are patients and their providers and their organizations, there are a couple things that we know are important. We have to think about the concept of connected devices. So even when we know that we're giving people devices that are connected, people don't always know what that means. So someone talked about informed consent earlier. How much do we need to tell people at the point of consent so that they understand what their device does, how it communicates, and how do they make meaning of that. They need to understand those risks and benefits.

We need to manage their expectations about the alerts and the information that comes with them. We need to manage what they really need to pay attention to and what they don't and how often. And, of course, we want people to pay attention to everything, but the reality is we know that people don't. So we have to really point them to the things that matter and are significant. And we talked informed consent already.

Then there's the other point of sort of alignment and communication. We have to

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

think about when there's a problem, that's when we have to communicate to people and think about what that crisis communication really looks like, and Jodi described well how the FDA does that. And who are the people that communicate with that, who has the expertise to explain it in such a way that it's understandable and meaningful and salient right now? And, of course, between the inventors and manufacturers, we have to talk about the actual evidence-based messaging, the training of providers who really often don't have any training at all or any information about this particular set of risks and the protocols for when to do that.

So I work in a lot of different health communication fields, and we think about just getting the information out to people as quickly as we can. So we often give people manuals with all the information they'll ever need to know about their surgery, their treatment, their procedure or their device, but they often don't need the whole thing right now, and so we need to think about how do we give it to people in chunks so they have the right information at the right time and they can use it then. That makes it much more meaningful.

So, in our life, we think about health literacy as a theory, a set of tools and processes, and what we can really help people do is understand the science and the risk, and I think that's what you want to do here. We want to apply the clear communication principles, we want to test all these materials with target audiences so that we make sure the messages really are connected and they work at the right time and place. And then we want to revise over and over and make sure the design and the content actually is meaningful. And if we do those things, we have effective products, media, and messaging, and it works on all platforms.

This is important because cybersecurity risk is not that different than any other medical risk. The stakes are high when something bad happens, but the reality is most of

the time nothing bad happens and people need to just go along and get along and use their devices. But when something happens, we have to be ready and we have to have the right messages, so we need to be thoughtful about that.

There are all kinds of health communication tools that are part of health literacy. But for the purpose of this, we're thinking about plain language where we start first with our purpose and audience. We want to think about who gets this message and what they need to know at each time point. So it's not the same message about cybersecurity always; it's what you need now and what makes sense. Structurally, how does that work so that people can process through regardless of their literacy level or their technology expertise? We have to think about the words and sentences and chunking those in such a way that they make sense.

In health literacy, it's important to think about behaviors and action steps so people have choice. I think that's been a great message today. As advocates and patient advocates, we think about just because someone tells you you have to doesn't actually mean you have to. You get to decide and you need to decide on the best information for you at any given time. And if we can think about presenting information with those behaviors and action steps, people can actually make decisions that are right for them, not right in the overall context of what someone said you should do.

We want to design these well, and in this particular case, we want to pay very careful attention to numeracy. People are being asked to respond to information on numbers that are well beyond their experience.

So the main things we have to think about is, in terms of uncertainty, we've got to acknowledge and communicate how much uncertainty there is. We're uncomfortable with this often in medicine. We want to make people feel comfortable, we want people to do what they're being advised to do and feel really high trust that is common in the medical

field, but the reality is, as we've heard all morning, we don't actually know fully with certainty how and when these things can happen.

And so we have to think about how to sort of communicate this. We can provide direct evidence with facts and numbers, and we should do that when we have that information. But we also need to think about the quality of evidence, so what's the underlying science or model? What is the meaning of the information that people have? Can we give them information that says with certainty that this is good information and you should pay attention to this versus information that's perhaps less good that they might get off the internet and some of the social media sites that aren't necessarily managed and processed in the same way?

And we have to remember that, from a public perception of risk perspective, we're often thinking more about the perceived magnitude of harm and less on the probability of that harm occurring. So we make all kinds of poor choices about risk, and one of the examples we think about in our office a lot is you can sit on the beach and worry about a shark attack and not pay attention to your sunscreen and get skin cancer, right? So in this case, this is really important, and we need to think about what is actually going to occur and what it means rather than just sort of these iffy things that don't have necessarily meaning.

But going back to our tangle of challenges, if we think about health literacy and communication that is clear and effective, we can untangle all of this and go from messages that don't work to ones that really make sense for people.

Thank you.

MR. CONWAY: Thank you very much.

(Applause.)

MR. CONWAY: We will now hear a presentation from Becton Dickinson concerning industry's perspective on cybersecurity communication.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MS. TAMARI: Thank you for giving me the opportunity to speak here today. We've heard from patients, we've heard from security researchers, sometimes patients and security researchers in one, government agencies as well, and so I'm going to talk a little bit from the medical device manufacturer perspective about that communication and coordination and what that really means, what does that look like.

And so at BD we have a coordinated disclosure process, and really, we want to try to make that as simple as possible, and the reason is, is once we get a risk or a vulnerability from either a security researcher or a third party, even internally, we take that pretty seriously because our customers are healthcare delivery organizations. They don't know how to secure -- if they don't know what a vulnerability is and what it looks like, they don't know how to lower that risk and eliminate it. And so it's our job to help them understand what that risk is and how they can then take that and use compensating controls and mitigating factors to help lower that risk in their particular environment.

And that process really looks like reporting, analyzing, coordinating, and then communicating. And I'll spend a fair time talking about communicating, but I wanted to walk through the reporting, analysis, and coordination of that piece as well.

So we accept reports of any sort of risk or vulnerability to a medical device through multiple means. The easiest is really on our website. We want to make it easy for people to find us and let them know that they've found something. So once they've been able to do that, we establish a sort of trust relationship. So we want to make sure to talk to these security researchers, they're bringing us valuable information, they're making our lives easier and, in turn, making healthcare delivery organizations able to better understand and assess that risk.

So we go through an analysis process, an analysis where we really look and we try to better understand what is this risk, what does it look like in our environment, what does

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



that impact look like. And we go through that clinical coordination of clinical risk assessment, and through that coordination process, we'll bring in other factors as well. It's not just done in a very siloed, organizational way. We really want to make sure to work with a lot of different partners. So we want to bring in the FDA, we want to bring in the folks at DHS, and really kind of come to an understanding and decide what does that communication look like because, really, at the end of the day, the healthcare delivery organization, they're not going to really look through the reporting, analysis, and coordination. They're going to get that final piece of paper, that final disclosure, and that's what they're going to see, and that's what we really need to kind of take a step back at and review what does this communication look like.

A lot of times our communication is filled with technical jargon and technical speak, industry speak that really the average, everyday individual may not understand. I personally do not have a technical background. I work in a very technical field, but I don't have, you know, a software engineering degree, and I think that is beneficial in the fact that it helps us ask the questions. So what does this mean?

And so when we look at what does this mean and how is language a barrier to our coordinated disclosure, I'm going to ask you to humor me with this next slide because in talking to some of my nieces and nephews, they use terms that I have no idea what they mean. They text message things that literally I don't understand.

So if we look at the first one, once you see what that is, Applebee's, it makes sense, right? The same thing for the second one, which is psycho. The third one I did for the technical folks in the room, a Konami code. The fourth is our Orange is the New Black. And the fifth is my personal favorite, bathroom emergency.

(Laughter.)

MS. TAMARI: So really the point of this slide is not to say we need to have an entire

coordinated disclosure in emojis, but we really have to understand what are the -- what is the language and the terms that the people who are receiving our message are using because that's the only way we're going to be able to get our message across. So what does that effective communication look like?

And at BD, the first thing we talk about is who's writing that message. So if we gave a coordinated disclosure to our R&D technical folks, nobody would understand it frankly. I wouldn't understand what they're talking about. But what we do have is we have a series of checks and balances to make sure that we really know what's happening. So not only will our R&D folks review that from a technical aspect to make sure things are technically sound, but we'll also have someone from communications review that to make sure that this is understandable. Can our healthcare delivery organizations review what the vulnerability is and then assess what that risk looks like? Which is where we bring in our clinical advocacy board. We have them review what does that look like from a patient perspective.

So when we talk about -- and we kind of heard some of these terms before when we look at impact, right? What does that look like for me as a healthcare delivery organization and then for my patient, for this particular vulnerability? And how can we then take those risks and lower them using any sort of compensating controls or actions that I can take?

And so using words like blacklist may work for our very technical audience, but instead can we use terms like, you know, filtering harmful websites? Does that make more sense? And so those are kind of the communications and conversations that we're having when it comes to how do we create our messages and who's writing that communication.

Also very key is knowing your audience. We have our bulletins for our healthcare delivery organizations, but that's not the only thing that we do in our internal process. Internally, we provide a lot of talking points and guidance to our service organization, right?

Our service folks, they're in the field, they are at the hospital site, they're kind of figuring different networks, and they're going through with the health IT space engineers. And so they need to kind of better understand what does this mean from a technical IT perspective. And so we also work with them to say what is -- who's the audience? We're not going to talk to them in the same way as we would talk to a health delivery organization, and we may merge the two, but we want to give them specifics for the things that they need. And so kind of talking that language is really key to reaching, really, that audience.

And, really, the next two kind of bullet points talk to each other, is how do we then get that information across? So if we have a coordinated vulnerability disclosure that we are releasing, how do we release that and make sure that the most amount of people see it? So we could publish it on our website, which is something that we do. But then how do we go through and reach the correct amount of people?

And this is really where our partnerships come in, where we work with DHS to make sure that our communications are aligned and we're coordinating at the same time to make sure that our healthcare delivery organizations get that communication. We also work with our information-sharing analysis organizations as well, so they can take that message and provide it to their audience. So it's not just, hey, you know, we've done this and we've kind of checked the box and put it on the website. No, we really want to make sure that message gets across so that healthcare delivery organizations can then take that, digest it, understand, and then lower risk for them within their particular environment.

And I think we do have an opportunity when it comes to education and media about some of these items simply because we've been using this technical jargon for so long and it seems terrifying and scary when you go through these messages. But the reality of taking the message and saying this is what you need to lower the risk, right, it's putting a lock on

your door. If someone came to me and said, oh, you don't have a lock on your door, well, here, this is what you need to do. I'm going to go out and get a lock and say, okay, I've just lowered my risk for someone to just waltz into my front door. So effective communication is something that we really look at when doing a lot of these coordinated vulnerability disclosures.

The second thing, and I think maybe the most important thing, is timely communication. Ninety percent of responding to a vulnerability is all about preparation. The vulnerability itself will change multiple times. I can't predict what the next vulnerability will be, but I can predict how I react to that.

And so our ability to respond to a mass vulnerability like WannaCry is directly related to how prepared we are. So we can take plans and make them for very specific scenarios, but that is not going to help us. We really have to take frameworks and take how do we communicate with each other and who needs to be in the room and what does the coordination look like, because that's really what's going to be key in preparing for these types of vulnerabilities and both, you know, on an enterprise level and within a device itself. That will allow us to say, hey, you know what, I know the person from R&D that we need to call, I know the person from our service organization, and pulling them all together and making sure that they're communicating with each other.

So it's really more of an exercise in cross-communication and coordination than saying here's a prescriptive plan for WannaCry. Really, it's how do we now deal with another WannaCry, something that's going to be similar but is going to be a little bit different as well? So what does that look like? And so we really say, you know, friends don't let friends make plans. We make frameworks for what this is, and we have incident vulnerability management plans at BD. And so, really, we kind of take that and we say what does this look like, what does certain risks look like in specific instances and in specific

products, and what can we do to kind of lower that risk. So that way, when an event does happen, we really are prepared when it comes to providing that communication, coordinating with our stakeholders, analyzing any of the information that needs to be analyzed and really then reporting it back to healthcare delivery organizations.

That's it. Thanks.

MR. CONWAY: Thank you very much.

(Applause.)

MR. CONWAY: We'll now hear a presentation from the Juvenile Diabetes Research Foundation (JDRF) concerning patient perspectives on cybersecurity communication.

MS. McCHESNEY: Good morning. Please excuse my voice. I'm having some seasonal allergies. But yes, I'm Karen McChesney. I was diagnosed with Type 1 diabetes in 1990. I hold a volunteer position of advocacy team chair for the New England chapter of the JDRF, and that's my conflict of interest disclosure.

So everybody living with Type 1 diabetes uses some kind of device as part of their treatment, the most common and basic being the glucometer where you're pricking your finger, putting it on a test strip to get the blood glucose reading, and many use insulin pumps or insulin pens rather than injecting with a syringe multiple times per day. And even some of these pens are becoming Bluetooth enabled so that the user can record doses throughout the day. So even our most basic devices are becoming more and more technologically vulnerable to cybersecurity threats.

Some with Type 1 choose to use continuous glucose monitors, also referred to as CGMs, and other systems that measure blood glucose levels, such as Abbott manufactures a device called the FreeStyle Libre. You might have seen those ads on television. It's not quite the same technology as a CGM. It's more of an on-demand reading where you swipe the device over your body and the sensor will give you a reading but not in a continuous

manner. And then also some people are using devices that close the loop between pumps and CGMs. It allows them to device and adjust insulin doses accordingly. For instance, your CGM will be trending up but the device knows your glucose is trending up, the device will give you a bit more insulin. If you're dropping, it will taper that dose that you're getting. A lot of patients are choosing to use off-label or non-FDA approved devices to loop, and then some are using the one FDA-approved Medtronic closed-loop system.

I know a lot of people with Type 1. I don't particularly myself use the Medtronic pump that was recalled, but I have a large network, so I kind of took an informal poll to figure out are people with T1D -- and they're Type 1 diabetics, T1D -- and their caregivers are really concerned about cybersecurity. Specific to the recall of the Medtronic pump, one father said, "This is about manufacturers wanting us to use newer devices," wanting us to buy their newer devices, since the Medtronic pump was an older one. And another said, "I took comfort in the fact that a potential hacker would need to be very close to me to gain access to my device," within 2 or 3 feet most of the time for that Bluetooth connectivity.

So the bottom line is that this is a risk that most are willing to take, and in fact, myself, another young woman with Type 1 diabetes who's in grad school, and a mother of a teen with Type 1 diabetes were sitting with Senator Markey's health policy fellow earlier this year and talking to him about funding for the special diabetes program, and we were showing him all of our devices. My friend was showing him how she could check on her Apple Watch her son's glucose level, which was up in Massachusetts at the time and we were down here. He was very impressed with it, and he said are you concerned about cybersecurity? And the three of us looked at one another, and we said not a bit. So the bottom line is that even though that these risks are present, the long-term effects of having consistently out-of-range blood glucose levels is a far greater threat to our health than these risks. Some have said there's more effective ways to harm someone if you really

wanted to, and that a child could accidentally give a larger dose of short-acting insulin or even an overtired Type 1 diabetic or their caregiver could do the same thing so that other risks are more common. In fact, I did that years ago. I was using injections, and instead of my long-acting 18 units, I gave short-acting 18 units, so I had to manage that throughout the day by taking in a lot of sugar.

But basically, you know, we're using these devices to really better our quality of life. Using a pump and a CGM is just a world of difference from when you're pricking your finger multiple times a day and giving injections. So the risk far outweighs -- I'm sorry, the benefit far outweighs the risk.

Another thing I thought about when approached to give this talk is where do we go to seek information on product recalls, cybersecurity risks, etc.? A lot of those with T1D have a very open relationship with not just their endocrinologists but their nurse educators or certified diabetes educators. Oftentimes these people can be reached the same day via email or cell phone, so that's someone they go to. Obviously, the FDA, the manufacturer. Many that I spoke with said that they prefer to read information put out by the FDA since they had no financial interest in the matter.

And another large source of information is the DOC, the Diabetic Online Community, which I find is becoming increasingly popular for Type 1 diabetics to receive real-time information and opinions from multiple sources. And I think speaking from the patient perspective, I enjoy just kind of the open candor, and nobody there has any interests or risk, really, you know; you're all giving information and tips as fellow patients where there's no liability, whereas a doctor might say I can't medically advise you to do that or not.

And, actually, like I said, the off-label devices, people are using these when they haven't gone to market yet. They've gone to market in other countries, but people are finding that they're waking up with their glucose in range, it's been in range all night,

whereas somebody who's not using a closed-loop system, my CGM line might look like this if I've risen and fallen throughout the night, which again leads to the long-term complications of living with Type 1.

And I was also asked to provide feedback on the information itself. Was it adequate? Was it clear? Was it timely? Everybody I spoke with said that they were able to locate the information quickly, easily, and they were satisfied; they felt confident after reading it to make an informed decision.

A couple quotes from the community:

"I read the Safety Communication provided by the FDA, and it contained all the information I was seeking. I made my decision and chose to continue with my daughter's current care plan, which includes a pump on the recall list, despite the risk."

Another Type 1 diabetic said, "I skimmed the information published by both Medtronic and the FDA and didn't find anything to be concerned about."

And lastly, "I saw that seven recommendations were listed 'to minimize the potential risk of a cybersecurity attack while you are waiting for a replacement pump.' I thought to myself that perhaps all of us using devices to help manage our T1D should do this." Those were things like be attentive to the pump notifications, alarms, and alerts, do not share your pump serial number, keep your pump and all devices connected to it within your control at all times, immediately cancel any unattended boluses, etc.

And most prefer to look up the information online. Medtronic did email any users that were on their lists as a current or past user of their product. Some prefer a hard copy. Many saw the FDA's tweet. As I said, I reached out to my network, and they said that that was where they first saw the information. I believe the information was easy to digest; the steps were clear. Always consult your medical professional or healthcare team and contact the manufacturer or the FDA if you have any additional questions. None of the language



used was panic inducing. I believe it was just very spelled out in a clear, non-alarming way as opposed to the headline of one of the articles I read, which was called "Excuse me while I turn off your pump."

And I think patients and caregivers of most intellectual abilities would be able to read the information and feel confident and informed to make a decision regarding their care. They know what to do or at least what to do next.

That's all. Thank you.

MR. CONWAY: Great, thank you very much.

(Applause.)

MR. CONWAY: I'd like to thank the FDA; the University of Michigan; the University of California, San Diego; Thermo Fischer Scientific; Health Literacy Media; Becton Dickinson; and the Juvenile Diabetes Research Foundation for their presentations.

Now we will have an open committee discussion and clarifying questions from the Committee. As a reminder, although this portion is open to public observers, public attendees may not participate except at the specific request of the Committee Chair. Additionally, we will request that all persons who are asked to speak identify themselves again each time. And I'll also ask my Committee members to do that as well. It makes it the easiest thing possible for the transcriptionist.

So at this point, does anyone have any specific questions for those who presented earlier this morning, here on the Committee?

Go right ahead, Monica.

DR. PARKER: Monica Parker.

My question is to Mr. Radcliffe, good guy hacker. The question I have -- and as a clinician, it kind of bothered me a little bit; he spent most of his time teaching his doctor about new things that he should be aware of with his device. Where does your doctor get

his information from besides you? Where would his colleague get his information if he didn't have you as a patient?

MR. RADCLIFFE: That's a great question, and I don't really have a specific answer for it. I know that my particular doctor goes to a lot of conferences, but he doesn't see a lot of presentations on cybersecurity risks from cybersecurity professionals. And maybe that's something that somebody like myself should reach out more to an endocrinologist community, just speak in those arenas as opposed to cybersecurity communities, which is where I spend a lot of my time speaking. It is something that we talk about quite a bit in the communities, getting outside of our echo chamber and to educate more people outside of there. But outside of that, I'm sure that he goes to the FDA website, I'm sure that the device manufacturers tell him about the things that are going on with their devices.

But to be honest, there is a very, very small community of researchers that work on medical devices. It's a very small community. So the body of knowledge that's there to distribute is still very small, which is another challenge for this particular arena. There just isn't enough subject matter experts to go out and speak at cardiologist events, at endocrinology events, at all of these different events where doctors get their information or nurses get their information. And I don't get a lot of invitations. I've gotten two invitations in the past 5 years to speak at those types of events.

DR. PARKER: They don't know that you exist.

MR. RADCLIFFE: Potentially not, yeah. Or how to get ahold of me, because both times I was very excited to speak at those events because it is an opportunity to speak to people who are actually directly connected to the patient, which is where I think that the focus should be to educate those people that are in front of the patient.

DR. PARKER: Thank you.

MR. RADCLIFFE: Thank you.

MR. CONWAY: Great, thank you very much.

Amye.

MS. LEONG: Amye Leong.

Thank you all, speakers, for your excellent presentations. I am struck by the area of knowledge upon development, upon innovation, to get it into the marketplace and into patient use. So I'd like to direct a specific question to Dr. Fu from the University of Michigan, if you wouldn't mind stepping forward, but really to those of you who have spoken to this and what you think the role of the FDA might be in this.

So my specific question to you, Dr. Fu, is I totally understand where you're coming from and where the science, the technology, the innovation, and as well with that, the responsibility of looking now in innovation and development and making lives of all of us easier, faster, quicker, more accurate, but looking early on, not later on, as you said, at the prospect of any kind of cyber intrusion or attack.

Where do you think this should go policy-wise? From an academician, someone who's in the business, in research, what roles do you think our academic centers should play, the innovation centers should play, a regulatory agency should play? Who needs to take the lead in these kinds of activities to help coordinate, to help motivate, to help even prepare the kinds of appropriate resources needed to combat these kinds of things? I would love your opinion about that.

DR. FU: Sure. So it's a complicated answer, and I don't have any silver bullets. I would say the main complicating factor is just how interdisciplinary the problems are.

MS. LEONG: Okay.

DR. FU: The two areas I view as challenging to bring together, the cybersecurity and then the delivery of healthcare, because there's very different training, very different kinds of mindsets.

In terms of agencies, I actually co-wrote some recommendations about -- I think it was about 7 years ago on a different advisory committee, the NIST Information Security and Privacy Advisory Board, the ISPAB, and they wrote a letter to then Secretary Sebelius on some recommendations on what agencies in the Executive Branch are probably most capable to have ownership of the problems and which ones should interact with each other. Off the top of my head, it would be difficult for me to list them all, but FDA and the National Institute for Standards and Technology (NIST) were number one up in there, along with DHS and some other agencies who have special expertise.

From an academic standpoint, I somewhat jokingly -- I'll give academic talks on the sort of 200-year plan to solve this problem, because if you look at hand washing, when folks like Ignaz Semmelweis did their original work in, what, the 1840s, and still we have problems with sterile technique and such, and so this is not the kind of problem that's going to be solved in a year or even a decade.

So to me, I think from an academic standpoint, it's about standing up the programs, to train the students. This is not about writing the next research paper, but it's really about how do we create the next legion of students who are going to become these experts who can bring together these two disciplines? And I'll tell you right now, it's very difficult because it's a lot of material for a new student, and it's very overwhelming. Oh, programming. Oh, and now I have to go into the surgical room, so I bring the students into the surgical room to get them to understand those kinds of challenges. Not many students are able to survive that kind of rigorous training. But I think the interdisciplinary nature is the most challenging. Does that cut to your question?

MS. LEONG: Very enlightening. Thank you, I appreciate it. Thank you.

DR. FU: Okay.

MR. CONWAY: Great, thank you very much. It's 10:21 right now, and just for

context for Committee members, we'll do a hard break at 10:35 for 10 minutes. But Katherine has the next question here for those who spoke this morning.

DR. SEELMAN: Thank you, Paul. This is for the group of people, so I have three different questions and depending on how much patience everyone has.

MR. CONWAY: So Katherine has three different questions. I'll tell you what, Katherine. What we'll do is we'll do your first question and the first speaker, and then we'll go to Lisa, and then if no one else has questions, we'll come back.

DR. SEELMAN: Okay. Dr. Tarver --

MR. CONWAY: Thank you very much. Katherine, can you bring the microphone a little bit closer to you?

(Off microphone discussion.)

MR. CONWAY: If you bring it a little bit closer.

DR. SEELMAN: Oh, okay.

MR. CONWAY: I think that should be better.

DR. SEELMAN: Is that better? Okay. Yes, the first question is for Dr. Tarver. Is she here?

UNIDENTIFIED SPEAKER: Oh, yes.

(Laughter.)

MR. CONWAY: Dr. Tarver's always here.

UNIDENTIFIED SPEAKER: We all got to get away.

(Laughter.)

DR. SEELMAN: Yeah, thank you very much for -- everybody, for really informative presentations. As we all know, FDA is a scientifically driven regulatory agency, and the question of appropriate and effective regulations for protection of users in a cyber environment is what we're talking about. So it seems to me that there are multiple points

of vulnerability in multiple regulatory jurisdictions and we really haven't -- I sort of see it as a dial phone almost, where you have a point of jurisdiction related to a vulnerability, and I haven't seen that today as much as I would hope to because, really, this is a partnership situation in trying to regulate these very complex matters.

In any case, one of the questions I have is medical devices at level three and your feeling about whether we need case studies of users of connected medical devices as they live their lives, not only in the health environment, which is of course more regulated, but outside that environment and that that would be very useful information for all of us. So that's my question for you.

DR. TARVER: So I'll start, but I think it's probably more appropriate for my colleague, Dr. Carmody, to answer. I do think that we talk about real-world evidence and how collecting data outside of the trial setting -- but in the real world can really inform our activities as a regulatory agency, as well as healthcare providers and the entire ecosystem. So the collection of data is helpful, and that potentially can inform some of those case studies where there are challenges with a particular device. But I will turn it over to Seth to answer the cyber portion of that question.

DR. CARMODY: Thanks, Michelle. I thought I got away with it for a second, but you brought me back in. Yeah, I think the idea of detectability is something I'm hearing here and that using real-world evidence in a cyber sense to understand what is actually happening out there is something that we've discussed and actually put into our premarket policy document, a draft version of that document that's public. It was October 2008. We know we can learn a great deal about what's actually happening observing that, and I think that will help us have a more granular conversation around what we actually should be paying attention to. Does that answer your question sufficiently?

DR. SEELMAN: Perhaps it's a beginning.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

DR. CARMODY: Sure. Yes, absolutely.

MR. CONWAY: Great, thank you very much. This is what we'll do, Katherine. If you can hold on one second, we'll have Lisa ask a question, and we'll go to Necie, and then we'll go to Kristina, and then we'll pick back up.

MS. GILBERT: I'm Lisa Gilbert. I have a quick response to Dr. Parker. When my daughter went in for her neurotransmitter, her neurosurgeon knew nothing about cybersecurity, so I was the one who educated him on that. So, certainly, that needs to happen.

But my primary question is for Dr. Dameff regarding informed consent. And my question was you mentioned informed consent takes place prior to going into the operating room when the patient signs that form with some education from the physician, and I was wondering what the full informed consent process may look like when it comes to cybersecurity. We had a later speaker refer to the stress that patients are under, making it hard for them to understand, and certainly, when they've got the idea and then they're signing the paperwork consenting to surgery, at that point that may be too late, I feel, for cybersecurity training. And, personally, I would like to see some cybersecurity training, just good, general hygiene practices for the patients far prior to the point where they're about to enter the operating room.

DR. DAMEFF: That's a great point. This is a complicated issue, so if we only rely on it to be delivered during an informed consent conversation, it's going to be woefully inaccurate or woefully -- we're not going to have enough time to talk about it in any meaningful way. So perhaps we should talk about a tiered approach to it. When you go to get a surgery, if it's not emergent, there will be discussions and meetings with their doctors before. They'll run various tests to make sure you're a candidate for surgery, etc. They'll talk to you about the procedure sometimes days, weeks, months before you have the

procedure. Perhaps having that conversation there would be ideal. It would allow for individuals who are not under duress of, you know, a surgery in the next couple hours, that opportunity to talk about that. That would be ideal. It's going to be hard. There's a lot of other things to talk about at that appointment. It relies on time for the appointment to do that as well as the physicians and clinicians being educated in that space. But I agree, this is definitely not the ideal scenario to just have it during the informed consent process immediately before but instead throughout the entire interaction with healthcare.

It's also an evolving thing, right? So just because you have a cyber informed consent discussion beginning with another device that you had doesn't mean that it will carry over to your next device that you have or that something won't evolve between those two spaces.

So I agree, it's not ideal. We should strive for a more longitudinal, less -- and there's also situations where it's just impossible. If you come into my emergency department and you're in third-degree heart block, a condition of the heart requiring emergent intervention, I'm going to put in a pacemaker, and our ability to have a long informed consent process where I can answer all your questions about cyber is very low.

MS. GILBERT: Understood.

DR. DAMEFF: And those types of things are going to be the exceptions.

MS. GILBERT: Thank you so much.

MR. CONWAY: Great, thank you.

Necie.

MS. EDWARDS: Necie Edwards.

And I want to thank everyone for your presentations today. They've been very informative and a real eye-opener for me. In addition to having fibromyalgia, I'm also a Type 2 diabetic, and my question is for Mr. Radcliffe.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



Mr. Radcliffe, I'm curious. Based upon your conversations with the physician, your own personal physician, have you identified any trends or the biggest takeaway from these discussions? And the reason why I'm asking is I, too, have had questions about my own device, and each time I have addressed this with my endocrinologist, she refers me to the diabetes educator. So one of my questions for you is who do you feel should be educating the physicians? And, also, is it the manufacturer? And what is your biggest takeaway from these discussions? Thank you.

MR. RADCLIFFE: Sure. Jay Radcliffe from Thermo Fischer Scientific and a Type 1 diabetic and researcher. I don't think that there is a single place that you get education from. I think that it's you get education from all of those places, you know, and while the doctor might have a lot of knowledge, I am very partial, because my mother was a nurse, to nurses having very hands-on and very direct care with patients. And, typically, they have the majority of the experience with the device. They're the ones that are outfitting the patient with the device, showing them how to use it for the first time, probably programming it for the first time. So I think that the bulk of the education comes from a diabetic education, a diabetic educator point of view.

That being said, when it comes time to ask questions from the patient, like this device connects to my cell phone, how do I know that it is safely transporting the information up to the internet? Most diabetic educators and doctors don't have the answer to that question. To be honest, most manufacturers are unprepared to answer those questions because it's usually a salesperson that you end up interacting with who knows the features of the product but doesn't have the technical answers to that.

And I see a lot of manufacturers preparing themselves to answer questions to their customer, whether that customer is the healthcare delivery organization or the patient themselves, and getting educational materials ready for them. Like we use encryption

when we send up data, you know, to the cloud, and we protect it with your password, and your password has to be changed, those types of things. So I don't see a specific area or a specific person that can kind of address those.

I do see the FDA helping with that. Most recently with their pre- and postmarket guidance documents, gives manufacturers the framework to say, okay, these are the things that we probably need to focus on and include. And I'll give you a short example of the updates, right? We jokingly had somebody say that they needed to update their iPhone for the last 4 months but they didn't feel like doing it. You know, we see a lot of healthcare manufacturers, a lot of hospitals kind of going the same route. Either they know they need to update it and they just don't, or they're not providing updates. And the FDA has made it very clear that there's a responsibility there to keep those devices up to date because that's a key component of cybersecurity hygiene.

So that's kind of one element of education. Maybe we need to educate patients. Similarly to how they have to update their iPhones, they have to update their medical devices. I know that on mine, I wear a continuous glucose monitor, and my Dexcom application will tell me, when it first starts up, you are out of date, you need to update, like every time. So they're very good about directing their patients to be up to date and current on those things. And I encourage manufacturers to do that, going forward, to help directly educate those patients on when they need to do those things.

MS. EDWARDS: Thank you.

MR. RADCLIFFE: Thank you.

MR. CONWAY: Great. Thank you very much.

What we're trying to do is land on time in respect to the public hearing side of this. So I apologize in advance to Kristina, Suzanne, and Philip. If your questions are not immediately pressing, we are going to have discussion later on today. At this point, what

we'll do is we'll take a break, and we will start precisely again at 10:45. When we return, we'll continue with the Open Public Hearing. Committee members, please do not discuss the meeting topic during the break amongst yourselves or with any member of the audience. And, again, we'll begin at exactly 10:45. Thank you.

(Off the record at 10:34 a.m.)

(On the record at 10:45 a.m.)

MR. CONWAY: It is now 10:45 a.m., and we'll go ahead and resume the Committee meeting, if folks can go ahead and take their seats. And if you want to continue the conversations, if you could do it in the hallway, we'd appreciate it.

We will proceed with the Open Public Hearing portion of the meeting. Public attendees are given an opportunity to address the Committee, to present data, information, or views relevant to the meeting agenda.

Ms. Williams will read the Open Public Hearing Disclosure Process. And out of respect to those who are testifying today, if those who are standing could please take their seats or move the discussions out into the hallway, we would appreciate it.

MS. WILLIAMS: Thank you, Mr. Conway.

Both the Food and Drug Administration and the public believe in a transparent process for information gathering and decision making. To ensure such transparency at the Open Public Hearing session of the Advisory Committee meeting, FDA believes that it is important to understand the context of an individual's presentation. For this reason, FDA encourages you, the Open Public Hearing speaker, at the beginning of your written or oral statement, to advise the Committee of any financial relationship that you may have with any company or group that may be affected by the topic of this meeting. For example, this financial information may include a company's or a group's payment of your travel, lodging, or other expenses in connection with your attendance at the meeting. Likewise, FDA

encourages you, at the beginning of your statement, to advise the Committee if you do not have any such financial relationships. If you choose not to address the issue of the financial relationships at the beginning of your statement, it will not preclude you from speaking.

FDA has received 11 requests to speak. The speakers will be given 5 minutes to speak. We ask that all individuals speak clearly to allow the transcriptionist to provide an accurate transcription of the proceedings of this meeting. Thank you.

I will turn the meeting back over to Mr. Conway.

MR. CONWAY: Great, thank you very much, Letise.

We have a number of public speakers today; therefore, I will go over the process again to ensure a smooth transition from one speaker to the next. When I call your name, please come to the microphone. You will have 5 minutes precisely, maximum, for your remarks. When you begin to speak, the green light will appear. A yellow light will appear when you have 1 minute remaining. At the end of 5 minutes, a red light will appear and your microphone will be switched off.

We will begin with a video presentation from Veronica Schmitt. Ms. Schmitt is unable to attend the meeting in person, so we'll go ahead and proceed to the video.

(Video begins.)

MS. SCHMITT: Hi, my name is Veronica Schmitt. I live in South Africa. I was diagnosed at the age of 19 with a full heart block as well as sick sinus syndrome as well as the conduction of my heart left much more -- or much less than what was expected of it. I was given a new lease on life when I received my first pacemaker. My pacemaker was a Medtronic pacer/ICD. It saved my life. But it's also piqued for me that, as a cybersecurity and forensics practitioner, I wanted to know more; I wanted to understand more. Asking my physicians these questions, I was left with blank stares and told that these devices are unhackable, un-fallible, and a hundred percent accurate. Trusting in my doctor, however,

being the scientist that I am, I still did my own research. I am both a patient and a researcher, but I'm also an advocate for patient rights. I have a saying and a philosophy that I live by: my device, my body, my life, my choice. I also describe myself with my device as beautifully broken and wonderfully flawed.

These devices evolved by humans. Humans make mistakes. Software fails. Devices are compromised. This is the world that we live in. Just because no one has publicly claimed it, it does not mean that it's farfetched. I think the work that I Am The Cavalry has done has shown that much. But the purpose for today's meeting and conversation that I'm having with you is to help you understand, from a patient perspective, what it feels like having to fight for your right to make a choice.

I have had a new device for 2½ years. My doctor never discussed with me changing me to a different model. That decision was taken for me; it was never discussed with me.

Soon after the device was implanted, I realized that I was passing out again; I was having flutters in my chest. I was admitted January last year into ICU due to a very low heartbeat. Even though my pacemaker tested correctly, everything was right, the doctor standing next to my bed watched as my pulse plummeted from 60 to 41 to -- my device never reacting. We reprogrammed the device, and again, no answers are given. I was made to feel like everything was in my head.

I then carried on. I ignored the symptoms. I decided that I did not want to feel like I was being ignored anymore. A year and a half later I started sleeping excessively, being tired, having angina, just overall the symptoms increased. Then we realized that the pulse rate that I had is either very high or very low. After a heated discussion with my new cardiologist, who was not the one that implanted this device, it came to light that indeed he would never have put in the device that I have in me now. For nearly 2½ years I had been walking with a device that is not right for my condition, that he programmed as best as he

could. But the decision was never given to me to be involved in the change of the model.

I think when vulnerabilities are disclosed to companies, they have a responsibility towards physicians to inform them. They have a responsibility towards me and other patients to let us know of vulnerability. But the responsibility is not just theirs.

Responsibility lies at the physician who a patient has a very trusted relationship with. We depend on you, the cardiologist, you, the physician, to advise us in the best course of action for our failing hearts. What we do not expect of you is to take decisions out of our hands. This is something that I feel very passionately about because had I had the discussion, things might have been a little different for me.

Now, physicians do not understand cybersecurity of devices. They do not understand software failures. For them, these devices are un-fallible. They depend on these devices to make interpretations for them. Medical practitioners are there to save lives. Cybersecurity people are there to secure lives. I think it's time that these two bridge the gap. There is a gap between manufacturers and patients, and manufacturers and physicians, and manufacturers and security people. There's the understanding from physicians that security is not important. Even though that is slowly changing, it's changing too slow. Medical device security is not a problem for tomorrow; it is a problem for yesterday, today, and tomorrow. It is an ever-evolving beast.

When a vulnerability is disclosed to an organization or a manufacturer, they need to investigate it. They need to engage with the researcher. They need to reach out to physicians with remediation options. And by this, I mean more than one option.

The physician then has the responsibility to reach out to their affected patients and have a conversation. Guide them, but the decision should be theirs to make. I want to highlight this. The device is implanted in their bodies. It is keeping them alive, supporting their bodies, but the decision about their life should be theirs. It should always be theirs.

I've been, given a choice, would have insisted on keeping a device that has lasted for 10 years, the same model. Why change what is not broken?

For a year and a half I have had to fight, I have had to argue, I've had to do my own statistical analysis because doctors rely on case studies. Doctors rely on statistics. There aren't statistics for cybersecurity problems in medical devices. It is a new problem, a problem that can only be solved when the manufacturers and the physicians and the FDA and the patients all work together. This is not a problem for one to solve. This is a problem that society needs to solve.

We need to take into consideration how a manufacturer remediates and responds to an incident or a vulnerability disclosure. We need to have the FDA look at how they deal with this incidence when they happen. Physicians need to understand what the impact on real life might be. Yes, there might be a 1% chance, but I am statistically that 1%, I have been my whole life, and I know that I would rather know that there might be something wrong that they are trying to fix than live in a fantasy world not knowing what is going on with a device that I depend on. And it should never be mistaken; this is exceptional tech. I am thankful for having this device.

What I am not thankful for is having decisions taken from me from physicians, manufacturers, regulators. Those decisions do not affect your lives, but they affect mine. Do not make the decision on life or death for me. Thank you for listening.

(Video ends.)

MR. CONWAY: The Committee thanks Veronica Schmitt.

The next person for public testimony will be Marie Moe. Marie Moe is also unable to attend the meeting in person, and I'll ask AV that if the video goes longer than five, to go ahead and stop it. It will be made available publicly. Thank you.

(Video begins.)

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MS. MOE: I am a security researcher, and I'm a patient. Every single beat of my heart is generated by a medical device, a pacemaker implanted in my body. Eight years ago I woke up lying on the floor. It turned out I had fallen because my heart had taken a break long enough to cause unconsciousness. So to keep my pulse up, to stop my heart from taking pauses, I needed to get the pacemaker. The slim device monitors each heartbeat and sends a small electrical signal directly to my heart via an electrode to keep it beating. But how can I trust my heart when it's running off of proprietary codes and there is no transparency?

When I got the pacemaker, it was an emergency procedure. I needed the device to stay alive, so there really was no option to not get the implant. There was, however, time to ask questions. To the surprise of my doctors, I began asking about the potential security vulnerabilities in the software running on the pacemaker and the possibilities of hacking this life-critical device. The answers were unsatisfying. My healthcare providers could not answer technical questions about computer security, and many of them hadn't even thought about the fact that this machine inside of me is running computer code. Little technical information was available from the manufacturer of the implant. This is why I decided to seek out this information myself.

So I started a hacking project, and over the last 12 years I have learned more about the security of the device keeping me alive. I discovered that many of my fears about the state of medical device cybersecurity were true. I learned that proprietary software that is not based on open standards and is not scrutinized by academics and researchers, the so-called security by obscurity approach can be hiding bad security and privacy practices and implementations when you look under the hood.

I've learned that legacy technology coupled with added connectivity equals an increasing tech service and therefore increased risk for cybersecurity issues that may



impact patient safety.

Security researchers like myself, we are not hacking the devices with the intention of creating fear or hurting patients. My motivation is to get the discovered flaws fixed. In order to do this, collaboration among all stakeholders is key. My wish is that me and other researchers get taken seriously by the medical device manufacturers when we approach them to report cybersecurity issues, that they have a coordinated vulnerability disclosure policy and invite me to collaborate, acting in the best interests of patient safety.

First of all, we need to acknowledge that patient safety issues can be caused by cybersecurity issues. It is not helpful keeping quiet about vulnerabilities, denying their existence. This will not make patients more safe. Claiming to be unhackable should not be a selling point. Manufacturers should instead collaborate in clinically open standards for a secure wireless communication protocol for their devices. Being transparent and releasing cybersecurity advisories to patients and doctors is something that makes me trust the manufacturer. It gives me confidence that they are taking these issues seriously and working to mitigate them.

Once a cybersecurity issue is known, it is important that all affected parties gets to read the information in a timely manner. Since many patients like myself are a hundred percent dependent on their device, a cost-benefit analysis needs to be made to weigh the medical risks in replacing a device or updating its software against the patient's personal threat model and exposure to cybersecurity risks.

In order for a doctor and patient to be capable of making decision assessments, all the facts need to be available and no information should be kept from the patient or the doctor. The solution going forward is transparency and better collaboration with understanding and empathy.

(Video ends.)

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MR. CONWAY: Thank you. Our next speaker is Zach Rothstein, Vice President, Technology and Regulatory Affairs for AdvaMed.

MR. ROTHSTEIN: Thank you and good morning. Thank you for the opportunity to provide comments during this public session. My name is Zach Rothstein. I am Vice President of Technology and Regulatory Affairs at the Advanced Medical Technology Association, also known as AdvaMed. AdvaMed represents manufacturers of medical devices, digital health technologies, and diagnostic products. Our members range from the smallest to the largest medical technology innovators and companies. We applaud the FDA and the Committee for hosting this meeting on what is for us a very important topic.

Patient safety is the number one priority for the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where technology constantly evolves.

AdvaMed's board of directors adopted five foundational medical device cybersecurity principles that serve as a commitment by our industry to ensuring medical device cybersecurity threats are addressed in a meaningful way. I'd now like to provide the Committee with a summary of these principles and describe some of our industry's related efforts.

First, a medical device risk management program should incorporate both pre- and postmarket lifecycle phases and address cybersecurity from medical device conception to disposal. We believe FDA has established a strong foundation for this principle through issuance of its pre- and postmarket cybersecurity guidances. Furthermore, the healthcare industry, through the Sector Coordinating Council, released a MedTech joint security plan which establishes a framework and maturity model to improve medical device cybersecurity.

Second, system-level security is a necessary component of an effective cybersecurity

strategy. To maintain system-level security, all elements of the system must be appropriately managed and secured because a system is only as secure as its weakest point. What this means is that system-level security is a shared responsibility. While device manufacturers play an important role, all stakeholders within the larger system must work together to ensure the system's integrity.

Third, we believe medical device manufacturers should support coordinated disclosure processes that provide a pathway for researchers and others to submit information, including detected potential vulnerabilities to the organization. We congratulate MDIC on the issuance of its report on this topic and believe it serves as an important tool to assist manufacturers to develop their coordinated disclosure programs. We are also happy to report that this year's DEF CON marked the highest turnout of medical device manufacturers within the conference's Biohacking Village, where device manufacturers and security researchers further established and built relationships.

Fourth, to enhance a manufacturer's ability to continuously manage their devices' cybersecurity, we believe the industry should participate in information-sharing bodies. Our members currently participate in various information-sharing organizations, including the Healthcare ISAC, or Information Sharing and Analysis Center. And AdvaMed recently launched its own information-sharing and analysis organization, also known as an ISAO, for its members.

Fifth, and our last principle, we believe that the development of consensus standards and regulations should continue to be conducted in a collaborative fashion that includes manufacturers, independent security experts, academia, and healthcare delivery organizations.

Again, we would like to thank FDA and the Committee for the opportunity to provide comment today, and we look forward to continuing to collaborate with all stakeholders on

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

this important issue. Thank you.

MR. CONWAY: Great, thank you very much.

Our next speaker is Benjamin West.

MR. WEST: Good morning, and thank you for putting together this venue for cybersecurity. I am currently employed by Dexcom, but I am here representing my own opinions, not the Dexcom opinions.

I started in 2009. I am also a Type 1 diabetes patient, as several of our previous guests have talked about today. I started in 2009 looking at my insulin pump, wondering what it was doing, getting frustrated about incidents that were causing me to go to the hospital, unintended visits to the hospital, needing rescue from EMR. And so I began looking at my pump, wondering what is this thing doing to me?

And what I discovered, as I started reverse engineering the pump, is that the cybersecurity that I had to overcome in order to get access to my own data was negligible compared to the burdens that were placed in front of me for getting access to the data, that even though it was fine for the manufacturer to create a system of security that was based off of security, that my access to my own data from the pump that I had bought was mitigated by proprietary loss, DMCA in particular.

And so that's my concern today is that as we talk about premarket versus postmarket communication of vulnerabilities, I'd like to invite us to take the opportunity to look more at the premarket side of cybersecurity.

And imagine for the Medtronic vulnerability, in particular with insulin pumps, imagine all of the confusion that could have been eliminated by allowing researchers, public, FDA, vendors to get access to the details that are needed to examine the quality of the security before that device was released. And so that would be my request today, is to go beyond data sharing to look at how can we assert beforehand that the issue of security

has been studied and researched before the devices go into the public marketplace?

My own work has focused on programs called Nightscout, called OpenAPS, sometimes called the DIY Loop, as an advocate for the We Are Not Waiting community, and I'm here to remind us that the benefits that the devices can deliver are life transforming.

There are people that are saying that I am taking advantage of the work that you've done to hack your own device to make myself more secure, to make myself more safe in a way that has been transformative, that this has been the biggest intervention in my life since starting insulin. And those are profound words to hear on something that has not been approved through the FDA, on something that has not been meeting the needs of patients.

And so, again, I would just invite us to look at that premarket phase before the devices are sold on the market, reconsider what it is to protect the property itself as well as the public safety and keep the public protected.

Thank you very much.

MR. CONWAY: Thank you.

(Applause.)

MR. CONWAY: Our next speaker is Dr. Nathanael Paul, Adjunct Professor at the University of Tennessee.

DR. PAUL: Hi. I was diagnosed with diabetes about 20 years ago. Started looking at patents about how these devices worked. About 10 years ago I engaged with the FDA about some of these issues. Before I go on, all my remarks and opinions are my own and no other private sector organization, and I should specifically point out later in this talk that I do oversee the security of a large medical device manufacturer now, as of a few months ago.

So what's happened recently? So Ben mentioned the recent news about the Medtronic systems. These issues have played out in the news repeatedly ever since we

notified the FDA, we notified affected manufacturers, and essentially, what's been unfortunate about this is, you know, the risk that's involved and sort of the messaging behind that, and I want to get to that in a second. So I've pointed this out.

So the specific risk that I'm talking about, essentially, there's two groups of affected patients that I typically think about. So the first is patients that are do it yourself or they've hacked the devices in order to behave in a certain way that improves their glycemic control. And then another group of patients that typically we might think of opting for worse forms of glycemic control over fear and misunderstanding of risk, and I think that that has a potential of happening. That was sort of pointed out about when the FDA might choose to communicate to patients. And, you know, I want to really sort of help you understand.

So I started closed-loop control in 2016. I actively advocated against implementing security controls within the do-it-yourself developers for specific reasons, and it allowed me to improve my quality of life. I view the security issues as being negligible currently with these implanted devices. I think it was correctly pointed out that as we increase connectivity and we have cloud-based repositories, that the security issues will grow. But I was able to basically share donuts with my daughter, which I hadn't really been able to in the past, and it was mainly because I was now able to better control my glycemia because of that.

And so what I want to leave you with today is just some observations and recommendations. So one observation is that a lot of times when people talk about vulnerabilities that they found, they do have financial incentives. Oftentimes they're going to be hired as consultants, some people take short positions in companies, and I think that's something to be aware of. So one thing I would recommend is that the FDA set up an independent review board or panel to assess risk and so that maybe that can help get ahead of messaging to patients.

The second thing that I'd like to point out is that a lot of these vulnerabilities, and I've discussed this, that yes, we talk about being high impact and low likelihood. The reason why we frame that, of course, is around risk and that is, of course, again changing with more connected devices. But for the vast majority of vulnerabilities, not just in diabetes devices but others, the benefit is so great in these devices that we should never take them away from patients. The biggest threat to my quality of life and my glycemic control is the reaction that we're now seeing in the market, right? So the number of devices that I now have access to, to use off label, of course, is now lessened because of what's been happening recently with manufacturers and the release of these vulnerabilities that are age old now.

So I want to advocate that we work with the DIY community. Don't shut it down; don't use a security vulnerability as an excuse to try to shut down DIY access. So I will assert that we can have both secure devices and DIY access.

And then I'm going to make a very specific request. Any medical device manufacturer that receives devices that might be associated with a vulnerability, I'd ask that the FDA allow them to redistribute those devices to patients that might be willing to accept that risk.

I'll even say that, you know, even up to this point in time; I've encouraged my endocrinologist, not even thinking about security issues because it's glycemic control that I think that's such a big issue. So it was mentioned, right, the shark and the sunburn. The shark here is the implanted device vulnerability, so sunburn is glycemic control and dying in your sleep from hyperglycemia.

So I'll end with, you know, let's make sure that we don't repeat mistakes of what's happened in the last decade with digital rights management around cryptographic keys and as manufacturers respond to implement security controls.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

So thank you.

MR. CONWAY: Thank you very much.

(Applause.)

MR. CONWAY: Our next speaker is Gretchen Riccardi.

MS. RICCARDI: That's your keyboard. My son's going to manage the computer for me.

MR. CONWAY: Great. If you could just state his name also for the record.

MS. RICCARDI: I will. Good morning, my name is Gretchen Riccardi, and this is Matthew Riccardi, my son. It's an honor to be here. I am so happy that you guys had this Committee meeting so that patients can have a voice into the FDA.

And I wanted to talk about that. Who owns my ICD? You know, is it mine? Is it my doctor's? Is it my device manufacturer's? Because, in practice, this really isn't quite clear and I was -- I have a bill of sale. Yeah, I have the record; I think it's mine.

So cybersecurity. Patients, we're passive recipients of telemetry sessions with programmers, so we're not necessarily aware of the programmer connecting to us. We have these built-in transmitters that open up the telemetry sessions, but unfortunately there's no, like, beep that tells me that I am actively communicating. Now, the programmer that connects to me at a device clinic or in surgery, it manages all aspects of the telemetry communications. So whether I am actively being interrogated, whether it is being reprogrammed or if there is some kind of hiccup and it goes into standby mode, all of this is kind of controlled with the programmer.

Now, patients don't authorize any kind of telemetry sessions with our implanted devices. We don't have a PIN that we're putting into the programmer, so there's really no way that we are taking control of the stuff.

Now, in the programmer, there is an end session and I believe, I don't have



confirmation, but I believe that this also ends the telemetry session with my device; it will close it down and put it back into a sleep mode. But the risk is when I go to the device clinic and a device tech just shuts the lid, turns it off, does not go through this end session, I'm left in the standby mode. And, well, there is a backup. Eventually that standby will time out, but if you think about where I am, I'm in a hospital and I'm in a device clinic. When my appointment is over, I am leaving and I'm going into a crowded elevator and, you know, I'm within the 15 feet of the long-range communications. So I'm just vulnerable at that point. So training is a big issue, and device techs really need to know to use this end session.

Now, the programmers themselves are not password protected. Now, there are some warnings in the manufacturer manuals about this, and it talks about making sure that the programmers are secured so that, because there's no password, anybody can use them, and they also contain patient information. You know, my PHI is on that device, and it's stored for a period of time.

So my point in going through this programmer is really what works well in the operating room is not necessarily what's appropriate for the device clinic. So you can see that the physician, kind of on the left-hand side -- I'm making gross generalizations, but on the left-hand side these are really physician functions when they are using a programmer in the operating room, whether to induce arrhythmia, to do a shock, and then over on the right-hand side is really the device technician functions. And who are device techs? They're nurses, they are people who have a 6- to 8-month certificate from either PrepMD or maybe ATI. So safety is a big issue with who has access to these controls.

Now, there is no role, it's the same programmer and there is no role, so the device tech has access to this induction test, this manual shock, and this rescue shock. So I'm vulnerable. You know, I have somebody who's connected to me, and I really don't know what they're doing.

Now, this is where patients need you guys' help. There's HIPAA law versus patient safety. I really don't have any idea of who is accessing my device. This information isn't printed anywhere. Am I connected to another device? Am I transmitting? The information just isn't there.

So, in conclusion, we really need the FDA's help in getting access to additional patient information. I currently have a HIPAA complaint. Let's all get together, let's talk to Roger Severino, let's talk to Administrator -- I'm sorry. Thank you all. I'm out of time, but I can talk later if you want to.

(Laughter.)

MR. CONWAY: Thank you both.

(Applause.)

MR. CONWAY: Our next speaker is Dr. Shantaram Rangappa. And I apologize in advance if I screwed up your name. From Deloitte.

(No response.)

MR. CONWAY: We know that he was here. We'll go ahead and rotate off and go to the next speaker. The next speaker is Dr. Reid D'Amico, biomedical engineer, medical device safety and cybersecurity/regulatory science, biomedical innovation and research/patient engagement, Duke and Vanderbilt University alumnus.

DR. D'AMICO: All right. Good morning, everyone. Can everyone hear me in the back? Great. So thank you to the Agency, the Center for Devices and Radiological Health, and the Patient Engagement Advisory Committee for hosting this wonderful opportunity to discuss medical device cybersecurity and the patient.

So I'm Dr. Reid D'Amico, and I'm a patient living with a rare genetic disease, and I use a medical device for about 3 hours a day as part of my standard of care. So today I just want to speak at a high level about what it is that I would want in terms of execution in the

event that I do have a medical device that has a risk that needs to be communicated. And I think it is worthy to note that as a patient with a rare disease, I have rarely found that my medical devices are even discussed at events like this.

So I have two things that I want to bucket out first. One is the medium of communication that I want to be contacted by, and the second one is the content of the communication.

So, firstly, I think that I would prefer that my first communication come through as a text message from my doctor's office, similar to an appointment reminder that I would get. So I just think about how I go through my day-to-day and emails get buried, phone calls I don't often answer if I don't know the number, and voicemails I don't often check immediately. And in this text communication, I would prefer it to say call the doctor, because I would want to connect with someone who's a human and who knows me well.

But when I answer or check my text message and let's say I'm in a meeting, I would prefer to have some sort of severity scale associated with it. One thing that drives me crazy as a patient is when I get a notification saying that I have new test result and I check the test result and it's either weird or it's out of range and my anxiety automatically goes up. So having some sort of green, yellow, or red severity scale associated with this text message would be great because if it were to come through as a text, obviously due to privacy concerns, it's not going to list everything there.

But it gets more complicated than that. So when I think about my specific family, for instance, my grandma has dementia and she also doesn't have a cell phone or email. So if the doctor were to call her, she probably wouldn't remember what happened in that phone call, and the same goes for a voicemail. So when I tried to talk to my grandma and explain to her what she would like, we came up with a letter actually being the best way to communicate with her.

So in terms of the content that I would want, I would want to hear as soon as possible, realistically possible, with the situation. And as I said, I'd like to hear from my doctor, someone that I know and trust, someone that knows the ups and downs of my care, and someone who can work with me in the event that, let's say, I'm traveling. And this communication, I don't want it to be overly technical, I don't want jargon, and I don't expect my doctor to be able to communicate the technical aspects of the risks. All I would want to know is (1) what do I need to do in order to mitigate the risk, and (2) in that very rare chance that I do feel that my risk has been exploited, what do I do as well?

The only time I really would prefer to engage with the medical device manufacturer is when the situation has evolved and is now under control. So, for instance, if the risk has been mitigated, now I just want to go in and see what the technical aspects are because I'm an engineer and I may want to learn something. Having some sort of website or portal on the medical device manufacturer's page would be really nice just to see what are the updates that are coming through, what is the cybersecurity posture of the medical device manufacturer, and also just as a patient, how can I remain engaged with the company as well?

So, in all, there are really just two takeaways that I have and one summary statement.

One, communicating with patients about risks is complicated, but there really isn't a wheel to invent here. Doctors already know the best way to communicate with their patients.

Two, in terms of the content, I would want to be told (1) what do I need to do to take care of this risk -- (1) what to do to take care of this risk, and (2) what do I need to do in the event that I do believe that I have been impacted?

And then the last thing I want to say is patients are an incredible asset and

stakeholder in this ecosystem. Engage patients often because our perspective is going to be a really critical ingredient as we figure this out.

Thank you.

MR. CONWAY: Great, thank you very much.

(Applause.)

MR. CONWAY: Our next speaker is Beau Woods.

MR. WOODS: Hi, good morning. First of all, thank you for convening this meeting. It is, I think, a testament to the number of people who actually care about patients and cybersecurity that we got -- this room is pretty much full, and I think that's really, really good.

I'm a little bit less excited about some of the conversations this morning that have seemed to pose a false dichotomy between security and patient safety or effectiveness of medical devices, and I think that's a wrong view, it's an old-fashioned view maybe, and partly it's the fault of, I would say, the security industry for failing to clearly communicate that the two things can go hand in hand. Partly, I think it's the fault of engineers for not making, you know, a lot of this stuff easy, but we'll get that figured out in time, right? This is not a permanent situation. I fear that if we don't keep pushing on improving security for patient safety and for clinical effectiveness, that we won't realize those benefits, that we'll have more potential risks and hazards for longer than they need to be out there.

I wanted to relate a quick story. I'm kind of accidentally here. My first job out of college was at a hospital, and at the hospital, when I first started working on security there, we had a situation where a number of physicians called me up. They said, hey, we're having some issues with our fetal heart monitors in the natal intensive care unit. About every 15 minutes or so they shut down, and then when they come back up, instead of telling us what's going on with the baby first, they have to display this window screen. I said, well, it

sounds like they have some kind of virus that's causing them all to reboot about every 15 minutes. So I called the manufacturer. The manufacturer said, oh, sorry, we can't do anything about that. It's malicious software. That's out of warranty, out of scope. They said even if we tried to do something, we'd have to get approved by the FDA instead before we could even deploy it to you, which was not true at the time and neither is it true now. So after working with them for a few minutes, they were unwilling or unable to help.

So, instead, I kind of put on my hacker hat, thinking like an adversary and thinking around the problem. Rather than trying to go through the established channels, I said you know, what could I do that could help the situation? So I built a plan with my boss at the time, we presented it to the CEO of the hospital, and essentially we were going to use the same method that the malicious software used to get on those devices to get it off. So hack into it, delete the malicious software, apply an update, and then see how things went. Effectively, the devices were broken anyway, so what's the harm, what's the risk? What we found is that the devices had a very old security vulnerability. We were able to very quickly get in and do all the things we wanted to do, and then the doctors were able to use those devices to continue providing, you know, the best care possible for those babies.

That wasn't the only time that medical devices were impacted by malicious software or by security risks in my tenure in the medical community, at the hospital, and it's not the last time that this has happened globally. A couple years ago when the WannaCry ransomware or malware hit 40% of UK hospitals and took them down for between a day to a week, there were certainly patient impacts. Now, it may not have been those that caused a smoking gun and we can tell that this patient died because of this security issue, but again, I'll call back to the earlier call for more statistical analysis to be able to look at patient security issues that come from cybersecurity. I think we need a lot more study in those areas. I think once we have that, we'll find that, of course, cybersecurity is integral to

patient safety, but I don't think we should have to wait for those empirical studies to be done to know that we have to take action.

So I'd like to applaud the leadership of the FDA in standing up several years ago, with their premarket guidance, the first round of premarket guidance, later the postmarket guidance and the most recent premarket guidance round, to effectively say this is an issue that we care about and we're taking it seriously. I think a lot of medical device makers, individuals within those organizations got empowered to do the things they already wanted to do anyway, and it's made us, I believe, demonstrably safer from a public health standpoint.

Thank you very much.

MR. CONWAY: Thank you.

(Applause.)

MR. CONWAY: Our next speaker is Andy Coravos.

MS. CORAVOS: Hi, I'm Andy Coravos. Thank you very much for having us today. I'm the CEO of Elektra Labs, and we work with pharma companies that are using connected products in their clinical trials, so we support people who are looking to collect biometric data remotely.

And one of the things that has been most interesting for me is the series of questions that we get as people evaluate these different types of tools. Often, people are very excited about how accurate they are, how usable, can you wear them in the shower, does it look like a prison bracelet when someone goes home. But very rarely do we get asked about the security of any of these tools. And something that's always struck me is how, I think, it's easy to put things in dichotomies. And so I think a lot of people are very excited about personalized care -- I am, too -- to have personalized care that also comes at the level of surveillance, and surveillance has a certain type of responsibility around it.

And so I'm really grateful that we have started having conversations around where we want to draw the lines around what we view as good and not good and the answers aren't always clear. So for many of these tools -- and I formerly served at the FDA's digital health unit, so I am very careful not to use the word devices because sometimes they are devices and sometimes they are not.

I think figuring out what we want to use, it's hard to draw the lines. And so one area where I am very glad that we are starting to draw some of the lines is around the infrastructure around what is good security and what is not and the baseline and then how we want to involve patient voice in that.

And so today I'm going to just talk about a couple areas where I think we're doing a really good job of convening different types of communities so that we have a broad area of perspectives.

So there's a group which many of you know, which is the Biohacking Village at DEF CON. This is a 501(c)(3) nonprofit, and it has a lot of security researchers. Security researchers, also known as white hat hackers, are those who do the work that we have seen today who really look at how we can improve these types of products for good.

In my work that I do with pharma, the word "hacker" has a pretty negative connotation generally, and people don't always know how to work together, and I'm really glad that in this last year the FDA has supported more and more of this community and started to attend these types of meetings and more people have started to come and convene together. I think initiatives like We Heart Hackers, especially even using things like a hashtag and involving the Twitter community, has been a really powerful movement and force.

I think there is also a number of different ways that we can think about how we tell the story. So one of the stories that has been really powerful for me is, as clinicians, when



somebody graduates from med school, they take a Hippocratic oath to do no harm. And so as these sorts of tools and devices start augmenting or changing the role of clinicians, should the software manufacturers, the data scientists, and others who build these tools also take a Hippocratic oath, and would that oath possibly look different than the oath that we have today?

And so there's a grassroots organization called I Am The Cavalry, which has started to develop the first Hippocratic oath for connected medical devices, and they've outlined a number of different security considerations in those.

And so we have different types of professional societies that doctors and clinicians can join. What are the professional societies that those who work in the digital area of medicine can also join? And so there's a professional society called the Digital Medicine Society, where more and more people are starting to convene.

And so if you can take away one thing, I think sometimes there's a lot of other -- like, you know, the regulators are others or the data scientists are others or the researchers are others, but we're all kind of starting to cross these different paths, and every time I hear somebody say that they're not technical, like, we're all technical now. Like, we're all interacting with these sorts of tools. And so I'm really grateful for having more and more communities where we come together like this and we start to learn that the others actually just meet.

And so if anybody has questions, I'd be happy to share more about these different types of communities. I think in many instances we're all beginners. I know that's kind of Buddhist about it, but I am glad that we're here and figuring out the different types of conditions that we want to have in building an intentional world together so that it can be safer for everybody.

Thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MR. CONWAY: Great, thank you very much.

(Applause.)

MR. CONWAY: Our next speaker is Nina Alli, U.S. Marine Corps, Executive Director, Biohacking Village.

MS. ALLI: I'm going to move the microphone because if I stand here no one will see me. So Nina Alli, Marine Corps veteran, Executive Director of the Biohacking Village.

So before I go into what the Biohacking Village is, that we all understand it, I want to ask a few questions. So who in the audience is a clinician, doctor, nurse, medical assistant?

(Show of hands.)

MS. ALLI: A couple. Caretakers?

(Show of hands.)

MS. ALLI: Engineers?

(Show of hands.)

MS. ALLI: Medical device manufacturers?

(Show of hands.)

MS. ALLI: Security researchers?

(Show of hands.)

MS. ALLI: Patients?

(Show of hands.)

MS. ALLI: Everybody. So everyone should be interested in all of this. Again, before I start, I want to tell you why I do what I do. So my parents, these are the emojis of my parents. So my mother was diagnosed with one of the rarest cancers in the world. It went from Stage 2 to Stage 4 in a week and went from Stage 4 to Stage 0 in two treatments of chemo. My father was a paramedic captain for the fire department of New York and was at 9/11, now has bilateral lung nodes as a result.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

So the Biohacking Village, for those who don't know, is a three-pronged approach to biohacking biomedical technical. We have a couple of different tracks. The first one is for talks. People can come in, talk about all the things that are security related. We also have the device village and the hands-on lab where people come in and get lessons on what security is, what they're doing, new devices. And the one that I'm going to speak about primarily for today is the device lab.

So what we do here is create a safe space for medical device manufacturers and security researchers to come together for interactions, share their findings if they haven't already disclosed them, discuss the issues that are being found from disclosures, and have pathways for better discussions.

The other initiative we have is We Heart Hackers. It's a strategic partnership with the FDA where we're trying to initiate medical device manufacturers into coming into DEF CON, which is the largest hacking conference in North America, to the Biohacking Village, to have those discussions, to have face-to-face interactions with security researchers so that they can have collaborative interactions and lead to better security.

Thank you.

(Applause.)

MR. CONWAY: Thank you.

At this time I'd ask my fellow Committee members, do you have any questions for the Open Public Hearing speakers? And if you don't, what I'd like to do is -- oh, I got you, Katherine. Go right ahead.

DR. SEELMAN: Now?

MR. CONWAY: Yes.

DR. SEELMAN: I just wanted to ask the consumer professional presenters whether they've run into any insurance problems in their work or any liability problems in their

work.

MR. CONWAY: So is there anyone who spoke during the public comment that would like to answer Dr. Seelman's question? Do you want to restate the question, Dr. Seelman?

DR. SEELMAN: Huh?

MR. CONWAY: Could you restate the question?

DR. SEELMAN: Oh, sure. My question is that during your activities as hackers especially, also as the patients, have you run into any insurance problems, insurance coverage problems in your activities?

MR. WEST: Are you referring to --

MR. CONWAY: And if you could just restate your name for the record? Thank you.

MR. WEST: My name is Ben West.

Are you referring to insurance covering like a replacement device or obtaining your first device? Is that along the lines of what you're asking? I'm just confirming. Is that the question?

DR. SEELMAN: It's certainly one of the -- are you a higher-risk person because you're on a connected device, and does that show up in your insurance coverage?

MR. WEST: So the insulin pump that I wear today I had to -- it's \$8,000 retail, so most people require insurance to be able to access that kind of technology. When I went to --

DR. SEELMAN: Yeah.

MR. WEST: When my warranty expired and I went to go replace it with a warranted device, my insurance company actually decided that I never should have been on this technology to begin with, and so they did not want to pay for a replacement device. That was resolved by appealing to the state insurance board after about 9 months.

MR. CONWAY: Okay, Doctor?

DR. SEELMAN: Yeah, that's very helpful. Thank you.

MR. CONWAY: Okay, Kristina.

MS. SHERIDAN: Thank you. Kristina Sheridan.

I have a question for Zach Rothstein, specifically around the five principles that are applied to the different organizations that you participate with. Specifically, the question is, around the principles that you have, how do you recommend that the organizations include patients around the decision making and think through communication to patients around the element of cybersecurity? The five principles that you outlined, they didn't clearly reflect how the patient was engaged within that. Are you looking to develop those sort of principles, and how are you approaching that?

MR. ROTHSTEIN: Sure. So one of the principles, I believe it's the first one, deals with the pre- and the postmarket aspects of medical device development, and in that premarket phase in particular, we look to what the FDA guidance says, and part of that FDA guidance, both the existing one and the draft of the updated version of it, specifically calls out the need to take into consideration the patient. And so in that medical device development process on the premarket side in particular, there certainly are FDA guidances related to this question. Similarly on the postmarket side, any safety communication would typically go through that type of analysis within at least the company level. So our principles do not necessarily call this issue out directly, but through FDA guidance and rules on the postmarket side, these issues are contemplated.

MR. CONWAY: Sure.

MS. SHERIDAN: Just one quick follow-up. So do you provide recommendations to your organizations in how to engage patients? Have you seen any best practices where people bring patients in such as this, for example?

MR. ROTHSTEIN: Sure. I can't think of any off the top of my head. We're actually

more of an advocacy-based organization. However, throughout the industry there are other organizations that might provide this type of information to our members.

MS. SHERIDAN: Thank you.

MR. CONWAY: Dr. Parker.

DR. PARKER: Monica Parker.

This is a question is for Mr. West. You had a question, you said you wanted access to details about the device operation before it gets to market, and I guess some of this comes from your response to the last question. But my question was what were the specific burdens that you were addressing, and what were the burdens that you encountered from hacking your device? I certainly understand that I need to have my device replaced, but now my insurance doesn't want to replace the device that was put in me in the first place. It's like, so what am I supposed to do?

MR. WEST: Sure. So one of the things that I've observed is that there's a certain progression of technology, the way that technology develops new features, the way that the market embraces those features, the way that those features are then priced or put into the market and then compensated for. So, for example, it's very typical in early stages of some technology to have something that's what we call hard coded. So, for example, insulin. It's known that insulin lasts somewhere between 4 and 6 hours for fast-acting insulin. A pump manufacturer might hard code the fact that this pump believes that all insulin takes 4 hours or 6 hours, right?

Now, we know that that might not be fully accurate, so the next generation of the device might get a new feature that says, you know what, instead of making that hard coded, let's make it personalized, let's make it customized so that you can get the right therapy for you.

So that's an example of the kinds of differences that I was looking to overcome as I

knew that the bolus calculator, the machine reading that produces and recommends every single dose that I take, doesn't offer me any justification to say yes or no for the suggested dose. It just gives me a printout, a grid of numbers, a table of numbers, and I have to say yes or no. So what justification do I have as a patient, much less as a doctor, to accept the suggestion from this machine, especially when the software that's in it may not be right for me? And so that's just one example of many, many, many examples where there's this promise of using personalized medicine, leveraging technology to get the greatest possible leverage we can for high-fidelity therapy. But that's not always accessible to patients.

And that's a technical burden that I ran up against, this idea that there's something hard coded in the pump that I don't have control over, that's not right for my body. The other kinds of obstacles that I ran into were actually policy based. When I approached the FDA I said, listen, I need -- I hear that you guys -- I approached FDA in 2011, 2012 asking, hey, I hear you guys collect documentation on how the device is manufactured. I've reached out to the manufacturer for them to explain to me how this device works, and they won't tell me how it works, claiming that that knowledge is proprietary. And so I came to the FDA and said, hey, I'm really interested in how this device works. Can you please share with me the details, the documentation that the vendor has shared with you, in order to help me make myself safe? And the answer then, of course, was well, we can't because it's copyrighted and FDA's authority does not extend to copyright.

And so I was unable to find out what are the basic details for how this device communicates with other devices, which is where the cybersecurity issue comes into play. And one of the things that I found out, despite the fact that it was proprietary, despite the fact that it was obscured, despite the fact that it was protected, was that there was very little to no security governing the privacy of my information or the safety of that information. And so that's why I focus so much on that premarket phase because that's

where if we can eliminate the protections provided for obscurity and using obscurity as a means for security, then the sunshine that that let's in allows the FDA to do their job.

And researching how the FDA works, I found that the purpose of collecting all of this information is (1) so that the FDA can provide oversight because it has essentially perfect knowledge of the marketplace, (2) as a tool for the vendor themselves to use to maintain and achieve quality. But really what struck me (3) is so that the process of science can happen and that the public experts and patients themselves could examine that same material for the same quality of fidelity and assurance and trust that the device is working the way it's supposed to. So those are a couple of examples, both therapeutic and policy.

MR. CONWAY: Thank you very much.

We have several other questions in queue, and we'll see how we do on time with that. We'll do a hard break for lunch at 12:15, but as we go through the public comment presenters, if there are no other questions for them, I'll ask commissioners or Committee members. And if there are still those who testified earlier this morning, we'll see if we can do a couple of questions there.

Having said that, if we can ask direct questions and have succinct answers, Amye, I'll go to you now, and then we'll come back over to Suzanne for those who presented this morning at the public comment here.

MS. LEONG: I'll try to be as direct as I can. We talk a lot about whether you're an individual hacker, through the experiences of those who have presented either this morning or late this morning or where collaborations have come in and hope to come. I'm going to turn the tide a little bit and ask about the darker forces. Are any of you aware of other forces, and I won't call them dark, but other forces for which there has been information where people want to hack larger groups of diabetic monitoring systems or other systems?

I say that in the example of a car manufacturer that has over the many, many years



reached out to a variety of different researchers in the area of biometrics trying to create that perfect driving wheel that would take your blood pressure, that would take all kinds of other telemetrics about the driver as a form of safety and that in the enlightenment of trying to improve those who have these kinds of conditions for which early warning signs might be important, particularly when you're driving.

I want to switch the tide a little bit and go the other way, the darker forces of a deep, dark web or any other area for which you might be familiar. Are you aware of any scenario where there are groups of legitimate or otherwise of entities trying to hack in or counterbalance or kill the development and the innovation of something that could be helpful, which is our subject today? Any information?

DR. PAUL: Great.

MR. CONWAY: If you can go ahead and identify yourself and your affiliation for the record.

DR. PAUL: Sure. Nate Paul, University of Tennessee, previously worked for the Oak Ridge National Lab. I'm going to give two responses to that. First is that any classified -- unclassified areas, I propose to use this offensively against nation state actors. The second thing that I'll respond to, that is I did teach a class in healthcare security last semester. I showed my students how, and I had one do it, you could actually identify all open-source DIY users basically. So Ben mentioned Nightscout. Across the world you could even look at sort of different ways they were using it, you know, all kinds, the spectrum of how the different systems that were being used were very different.

What was interesting was if you advance this attack one place beyond that, if you could find a vulnerability in the Nightscout implementation of a server, you could then do an at-large patient attack on the entire patient population.

What's also interesting, if you look at recent -- well, not recent research, research

that's about 7 years old -- you could actually start directing this to individual patient attacks. For example, you only need basically two to five blood glucose values in order to directly attack a patient.

The reason I wanted to bring this up is that we have now crossed that threshold where we do have risk with respect to the larger patient population, but I do not know that it's actually been used, but I now have a source code by one of my students, and a lot of these sort of look at where the different patients are.

MS. LEONG: Frightening information, but thank you for sharing that with us. Thank you.

MR. CONWAY: Great, thank you very much.

Suzanne.

MS. SCHRANDT: This question, it's really for any of the patient or consumer folks who testified but maybe most specifically Dr. D'Amico -- am I saying that right -- because you gave such specific examples of your own experience as a rare disease patient. What I'm struck by from what we heard this morning versus what we're hearing later this morning is earlier today I was getting this theme that there were purveyors of information about risk and especially when a risk is imminent or something bad has happened, a cybersecurity threat has happened, and those purveyors of data of information are the FDA, Homeland Security, MDMs, sort of the people in the know, and then they would give the information to the patients. And it seemed like that was a really artificial and worrisome linear relationship when, in fact, there should be patients involved on this side as purveyors of information themselves, and we're hearing about all these very activated patient groups that are involved in sort of deconstructing technologies and looking at threats.

So I'm actually curious about have you or have any of the other folks who testified ever been involved either with the FDA or with individual device manufacturers when a

threat has emerged and thinking through how to communicate to patients, thinking through what the remediation should be so that it's something patients can actually do? Does that question make sense?

DR. D'AMICO: Yes.

MS. SCHRANDT: Have you actually been involved sort of in the solution part of that, of the communication?

DR. D'AMICO: Yeah. So for me specifically, my disease state doesn't have any medical devices that have been impacted by a risk or no risk has been communicated. However, from the standpoint of patient communities, so for the cystic fibrosis community, we actually can't be in person because of cross-contamination, so we have a very strong online presence and online community, and usually when there is a hot topic within the field, we'll come together usually under the Cystic Fibrosis Foundation, so there's a patient advocacy group that houses us and our voice. That's usually how we all come together to create a mission forward.

MR. CONWAY: Great, thank you very much. For other presenters here at the public hearing, any other questions for those before we move into some of the morning presenters?

(No response.)

MR. CONWAY: If not, I'll go ahead and ask one. If I can ask Nina Alli to come back up for a second.

(Pause.)

MR. CONWAY: Good morning.

MS. ALLI: Hi.

MR. CONWAY: In some ways this is a follow-up question to a question that Amye Leong posed about "dark forces." So you, in your role, based on publicly reported

information and nothing from a classified source based on your background, but if you had to weigh your concerns of what might keep you up at night, how would you distribute the weight between state actors or among state actors, non-state actors, and the rogue individuals in regard to cybersecurity and medical devices?

MS. ALLI: So China and Russia in particular have --

MR. CONWAY: Can you speak into the microphone?

MS. ALLI: Sorry, I'm really tiny for one.

MR. CONWAY: I understand.

MS. ALLI: Is that better?

MR. CONWAY: Perfect.

MS. ALLI: Okay. China and Russia have decriminalized hacking and brought them into their government, so they act on the behalf and behest of the government. So that's something to take into consideration. And one of the other items is they are starting to teach this at very young ages, hacking security in middle schools and elementary schools in other parts of the world and in the country. They are engaging them very early, engaging students very early and bringing them into the hierarchy of security and hacking in those countries. So that's what keeps me awake at night.

MR. CONWAY: So that keeps you up. But if you had to distribute weight among state actors, non-state actors, and rogue individuals -- and I would assume, I don't want to put words in your mouth --

MS. ALLI: Right.

MR. CONWAY: -- but are you saying that the institutionalization of elements within a foreign government, if the activity has been decriminalized, I guess you would consider those state actors then?

MS. ALLI: Yes.

MR. CONWAY: Okay. So now taking a look at, in total across the spectrum, state actors, non-state actors, and rogue individuals, what would you say keeps you up at night as a professional and as a patient?

MS. ALLI: The resources that the nation state actors have at their availability: resources, computers, people, knowledge.

MR. CONWAY: Okay, thank you very much.

MS. ALLI: Yes.

MR. CONWAY: Appreciate it. Now what I'd like to do, we'll do a hard break in about 14 minutes for lunch, but I'm interested in coming back over the list of people that I had pending right now for questions to this morning's presenters. Philip, I have you. I know that -- my apologies. Bennet, I have you. I have you, Philip, first. Then I have Bennet, and I know that Katherine had one remaining question. So my apologies, Kristina, you did too. But, Philip, go right ahead.

MR. RUTHERFORD: My question was for Dr. O'Leary. Dr. O'Leary, you mentioned that health literacy was a precursor to -- is Dr. O'Leary here? Oh, good. You mentioned that health literacy was a precursor to beginning to have some of these conversations about cybersecurity, so I'm curious what your prescription is for sort of bringing up the sea level of health literacy to begin to have these conversations. And I say that because I think, as we're having this discussion, this is sort of the tip of the spear or top of the iceberg kind of discussion, and we're talking about things that I think everyone in this room has some awareness of the problem, but when I think about the people that I work with and just sort of the public at large, I don't know that there's this level of awareness or concern. So what's your prescription for fixing it?

DR. O'LEARY: Well, thanks for asking. I think one of the things that confuses people about health literacy often is that initial definition that we hear that's on the record from

government sources because it was first out of the gate here, but there are about a hundred other definitions that people who actively work in health literacy think about and use. Most of those are not deficit focused on patients, so the idea that patients are responsible for figuring out all the gaps and everything they know at the worst moment in their life, to figure out care in a context that is really out of their control is pretty unreasonable.

So I'll start there by saying health literacy, as I think about it, is in the much broader definitional context of the patient certainly as the center of their care and health situation, but also it's their providers and the organizations and assistants that work around them. And so if we start with all of those people together being responsible for sharing information in a way to make it usable, that's step one. And I think a lot of the conversations here that we're having this morning talk about that, people are talking about, you know, training providers to be able to have conversations, people are talking about the messages that they use and sort of the right timing of those messages.

So as I mentioned this morning, from a health literacy perspective, we need providers to know what they need to know, which isn't the universe of information about cybersecurity. It's the very specific how does cybersecurity affect this device that I'm advising for you right now? What could possibly happen? What do you need to know to protect yourself? When do you need to know it? How are we going to keep following up? Every time we see you, what do I need to remind you about and check in on and how do we sort of move each other along in that way? They need to know those pieces but not sort of all of the other real complexities of the ever-changing system of the cybersecurity landscape. And the patients need to learn along with them. And if we start in a place of trust and patients and families can ask the questions, bringing their whole families along to think about who in my family sort of knows a little bit about this, who's going to be my

caretaker, how are they going to help me do this? When do these decisions matter, that helps a lot too.

And certainly there are lots of manufacturers in the room who are thinking about this every day and very much are the experts in how this actually works and what the real risks are. And from a financial and legal perspective, they probably carry the most risk and have the most sort of skin in the game to think about it. And so if we can help them find a way to work with the regulatory bodies to figure out what the communications are and when and what the real risks are, I think you can go a long way towards spreading the responsibility for the health literacy challenge so it's not just about the patient having to figure it out at every moment. Does that help?

MR. RUTHERFORD: Yes, thank you.

DR. O'LEARY: Sure, thanks.

MR. CONWAY: Thanks, Philip.

Bennet.

MR. DUNLAP: Hi. My question is for Dr. Carmody. I'm looking at your Slide 3 and your Slide 7. Slide 3 says cybersecurity is the process of preventing unauthorized access, etc., which implies that someone is authorized to give that access. So the fundamental question that I have is who gives that authorization? Whose data is it? Who can authorize use? Who can authorize modification, access to stored information, etc.? Whose information is it? And then I'll follow up depending on what you have to say.

DR. CARMODY: Sure. So it's not the purview of the FDA to define who is authorized and who is not. It's really a combination probably of, you know, with the disease that you're trying to cure or treat, diagnosis, or in some fashion like that and collection of, you know, what physicians need and what patients need. So we'll call it user requirements or that kind of flavor. So who would be involved in sort of those types of decisions, who would

be involved in that process, that's who should be authorized.

And I think the example that I'll use is -- I think you brought it up around like the tech. If they're not, you know, authorized to do some treatment decision, they should not have access in a user role for a programmer; they should not have access to that, right? So in terms of like a granular example and thinking through user roles and requirements, that would be a good example, like who should have access to that type of functionality. Well, it could be your physician most likely, not the tech. So how do you think about logging into the device and then granting access or user roles around that? Does that help answer your question?

MR. DUNLAP: Well, so based on the public comments that we just had and the people that were patients presenting, I kept a little score. Every single one of them seemed to say it's my data. And I look at your Slide 7, and you have all these entities that encircle the patient and shield them, but the patient's not really part of that loop, and what I'm hearing loud and clear today, the answer of whose data is it, it is the patient's data and the patient with their physician can decide what to do with it. So if you create a system or you allow a system to come to market that doesn't allow the patient to access your data, you failed in your very definition of cybersecurity to the person who is authorized --

DR. CARMODY: Sure.

MR. DUNLAP: -- to act on that data is the patient and you've approved a system that doesn't allow the patient to act.

DR. CARMODY: So with respect to that, yes. So we're here today to talk about what patients need in terms of cybersecurity communication. So as far as they need access to data in order to communicate effectively what the cybersecurity issues are and how they should react, certainly they should have access to whatever they need. I can't speak to --

MR. DUNLAP: So if I have a pacemaker and I don't know that -- you know, I have this



real simplistic model, it's either transmitting error, it's not working right, or everything's okay, but I'm precluded from seeing that data process through some --

DR. CARMODY: Yeah.

MR. DUNLAP: -- linked cloud process that only lets my physician and the manufacturer and third-party researchers at their lab see it, I don't know that I'm flashing an error, and quite frankly, I'm the only one that needs to know.

DR. CARMODY: Yeah, totally agree. We had a conversation with a family around an update that was issued to a suite of devices. The update failed. They couldn't even get basic information off the device, it had no LCD screen, in terms of versioning number or what was actually going on with it. So I think in terms of how do we enunciate when there are issues or what the issues are, we certainly have work to do. To your earlier point, that's why we're convening this very panel. I didn't get up here to explain that I have all the answers, and that's why we're here today.

MR. CONWAY: Thank you very much. I'll tell you what, we have about 7 minutes. I have two other questions coming around the corner here, and Kristina, if I could, can I ask Rajiv to ask his question first and then we'll come to you? Go ahead.

DR. RIMAL: Thank you. My question is for Christian Dameff. I was fascinated by your take on informed consent this morning, and I just had a follow-up. You mentioned that we don't have the data to quantify the risk when we're talking about consent, and I just wondered, do we really have the data for most other things about which we're trying to calculate risk? And I was also going to talk about how this is not a normal distribution, that you've got small probability events that can cause havoc. So I guess my question is to what extent is the knowledge about that sort of absolute level of risk necessary in having an intelligent informed consent discussion? And is there harm in saying we do not know what those risks are?

DR. DAMEFF: A great point. I think there are definitely some things that we have great data on. For example, I cited blood transfusions, we can look at millions of blood transfusions and look at rates of subsequent infection from contaminated blood. But you're totally correct; there's a vast majority of the risk that we're trying to convey in which we don't really know the numbers or we're speculating or we're using the physician's expertise and prior experience to help inform that conversation and that process.

To answer specifically, I think that we have to say we don't know the risk, but I think the communication is so important. What I don't think is a good idea is to say because we don't know the risk, we don't communicate it. It's key. And we've heard these stories time and time again from patients. I had an incident, I was in the hospital for a while, and when I was leaving, they handed me a box. They said hook this up to your router at home, and it's going to communicate with your device, and they realize only at that moment that they are now part of the internet human of things.

Even though we don't know the risk, we should be able to have the conversation that there is a risk that we cannot calculate, we don't know today what that means, and that it can change. I think that's key. Right now we can say we don't know anyone who's been impacted by that, but that could change tomorrow and that component of that conversation, that this risk can change, is different than traditional epidemiological data, right? We know what the rates are; it's probably not going to change next week. Cyber's very different.

MR. CONWAY: Great, thank you.

Kristina.

MS. SHERIDAN: Yeah, thank you very much. I have a question that's actually for Jodi Duckhorn. So thank you for describing the communication process and the various communication that's coming from the FDA and the approach that's used to do that.

I managed my kids' health, especially when they were in crisis and they were in significant times of burden. It became very difficult for both my husband and I, so it's a very overwhelming process sometimes. There's not a lot of time in the day to do much of anything other than taking care of them moment by moment.

The information I got from the FDA was great, and I specifically signed up for the things that I think would be relevant and would potentially impact them, but finding the time to skim through that information and identify what was relevant to them in that moment was very time consuming, and I would try and do it, but it would often get slipped on the priority list because of other things.

So my question is, with the current approach and the future forward-looking strategy, how is FDA looking to be more targeted very specifically to reach the patients who are impacted by the events that occur, whether it's through use of unique identifiers for the devices, more informed tracking of that to be able to really pinpoint and get me the information I need to know that my child's at risk at the moment that I need it?

MS. DUCKHORN: So I can't speak to tracking at this time, but I can tell you that we do message testing to make sure that our intended audiences are understanding the messages that we're putting out. So in your case, if we're looking specifically to caregivers of children or caregivers of an elderly population, we would conduct message testing either on an internal FDA panel or on an external panel to make sure that these messages are understood. We also just recently translated this Medtronic safety message. So if there's a message, for example, that's specifically targeted maybe to a minority population, we can conduct message testing there or, again, do some translating depending on what the language is.

MR. CONWAY: Great, thank you very much.

At this time I'd like to thank all of those who testified in the public testimony and for

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

your willingness to share your experiences and your perspectives with us today. Your feedback will help us assure that the needs and experiences of patients are included as a part of FDA's deliberations on complex issues involving the regulation of medical devices. We sincerely appreciate your time here, what it took to be here, and the investment of personal resources to come and participate within the process. I now pronounce the Open Public Hearing to be officially closed.

We will break for lunch. Committee members, you're reminded, please do not discuss the meeting topics during lunch amongst yourselves or with any member of the audience. The meeting will reconvene in this room at 1:00 p.m. At that time I'll open the floor up for open public discussions, and I'll invite you, the audience, to participate in a roundtable discussion focused on the scenario you selected from the bowl this morning when you signed in. FDA staff will moderate the roundtable discussion and will be taking notes.

I would like to remind you that Committee members will not be a part of this discussion. After I open the floor up for open public discussion of the scenarios, I will excuse myself from the room and rejoin my Committee members. The Committee members will reconvene in this room 10 minutes before the roundtable discussions conclude at 1:50 p.m. I will ask that all Committee members please return on time. I would like to reiterate that the audience is to reconvene in this room at 1:00 p.m. You are encouraged to review the scenario during lunch. Please take any personal belongings with you at this time. Thank you.

(Whereupon, at 12:15 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(1:04 p.m.)

MR. CONWAY: It's now 1:04 p.m., and I'd like to go ahead and resume the Committee meeting. We'll begin with the roundtable discussion portion of the meeting. You, the members of the audience, can discuss a theoretical scenario regarding a cybersecurity safety concern associated with a medical device.

Every table member should have received a copy of the scenario. Each table will have the opportunity to discuss the question and comment according to your FDA table moderator's instructions. Your active participation and thoughtful comments are important. We encourage engaged and open discussions as you participate in this exercise. Your comments will be aggregated with all the comments generated by your table and will be presented to the assembled group, including PEAC members.

The scenario to be discussed is found on the paper entitled "Cybersecurity Scenario" that you picked up from the registration table. The tables will have 1 hour to discuss the scenario. There are no right or wrong answers to the questions, and the FDA is interested in hearing each one of your perspectives. FDA staff will moderate the discussion, and an FDA representative at each table will be taking notes.

When I and my fellow Committee members return from lunch, I will ask the FDA moderators to present the comments generated by the table members. While the actual roundtable discussions will not be webcast and will not be transcribed, the summaries from the roundtable discussions will be webcast and transcribed.

We are especially encouraging all patients and caregivers in the audience to contribute to the discussion. FDA attendees are welcome to listen to the discussion.

I'll now excuse myself from this roundtable portion and turn it over to FDA to begin moderating the scenario discussions.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

One final note: We did this exercise in the same manner in 2018, and the content of those summations by the Committee, from the Committee's perspective, were invaluable and quite helpful. So please be vigorous in your engagement. We appreciate it. Thank you.

(Roundtable discussion.)

(Off the record at 1:07 p.m.)

(On the record at 2:00 p.m.)

MR. CONWAY: Okay, folks, we're going to go ahead and start up. It's now 2:00 p.m., and the Committee has returned, and I'd like to go ahead and resume the Committee meeting.

We'll now begin our roundtable summations. I would like to go ahead and ask the moderator for Table Number 1 to summarize your table discussion. Actually, my apologies. Hold on one second. I'm jumping the gun, Doc. Before we begin the roundtable summations, what I'd like to do is go ahead and give FDA the opportunity to do two points of clarification based on the discussions this morning.

And go right ahead, Suzanne.

DR. SCHWARTZ: Yes, thank you. Thank you very much, Paul. This is Suzanne Schwartz from CDRH, and based upon the discussion that took place this morning, we wanted to offer a clarification from FDA's perspective. There was a question that came up with regard to cybersecurity as it was defined as a key term on the FDA slide, and that was described as a process of preventing unauthorized access, modification, misuse or denial of use or the unauthorized use of information, etc., etc. Two concepts got conflated here, and we want to clarify those, so I'm going to start with one aspect, which is the security functionality aspect, and then Michelle Tarver is going to explain the data piece so that it's clear what FDA's position is.

When we are talking about this from a cybersecurity perspective, through the lens of

protecting a device from being exploited, from being attacked or there being any kind of intrusion, we are speaking about the performance, the safety, the functionality of that device and not being impacted. And so when we say an unauthorized user, unauthorized access, it's someone other than the patient, a healthcare provider or caregiver, someone who has been authorized in the use of that device.

And the lens through which we are defining cybersecurity here is with that framework in mind, that the integrity of the functionality of that device, the availability of that device to perform as it's supposed to perform, as well as the confidentiality of data, what's often called -- I said it in reverse, but the CIA triad, confidentiality, integrity, and availability, is properly preserved. So that's how we are scoping it with regard to cybersecurity from a safety and performance perspective, and Michelle is going to speak about that, FDA's position, from a data perspective.

DR. TARVER: So Michelle Tarver, CDRH.

So we want to make it very clear that the data that's collected by medical devices belongs to the patient. There's a guidance document that we issued in 2017 that speaks directly to that, that clarifies that the data that's collected by the medical device belongs to the patient and they should have access to it. And so we want to make sure it's very clear that when we're talking about data, that your specific data is your specific data. So it's not owned by another entity that you have to purchase it from. And so we just want to make sure that that also is not lost in the discussion. Thank you.

MR. CONWAY: Great, thank you very much, especially for raising the 2017 guidance and making yourself available for the clarifications.

What I'd like to do now is go ahead and have the summation of Table Number 1.

DR. BENZ: Good afternoon, I'm Heather Benz, FDA.

Question 1 was "Would you expect your healthcare provider to discuss the

cybersecurity risks associated with Device C during the informed consent process before surgery? Why or why not?"

Because the doctors have an active patient relationship, this would be expected. However, the doctors may not be equipped at this time to have an in-depth conversation. Additionally, patients, during the informed consent process, may have a lot of information presented to them and may not have the ability to recall it all. Therefore, the focus was on the right amount of information at the right time and access to more information that patients could follow up on as they have the bandwidth, you know, in terms of anxiety and information retrieval.

There were concerns that physicians may not receive sufficient training to communicate effectively about cybersecurity. Therefore, they may not be the best place to get the most cybersecurity information. There was agreement that the risks should be raised. If they are not well defined, it is better to state that rather than to skirt around the issue and sound "sketchy." So because physicians may not have all the information at hand, they may want to point patients to a manufacturer's site that may have more information or other resources.

Overall, in context, there are bigger concerns at the time of the informed consent about the surgery, about the effect on quality of life, about where the patient is in their disease. And health literacy may be variable, so it may be hard to understand the details. Therefore, while it should absolutely be mentioned and information should be provided about how to keep yourself safe, there's need to know versus nice to know that should be clear.

Thank you.

MR. CONWAY: Great, thank you very much. Does anyone else from Table Number 1 have any additional comments to provide?

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



(No response.)

MR. CONWAY: Great. Barring that, I'd like to go ahead and ask for the moderator from Table Number 2 to summarize your table discussion.

DR. ROSS: Good afternoon. So at Table Number 2 we were discussing whether the possibility of the device being vulnerable to unauthorized access and interference would change the decision to have the device implanted. And at our table, we discussed a variety of issues, and one of them was really just, from a patient perspective, in a lot of instances there could be the baseline assumption that if the FDA approved it, then, in general, the device has a better benefit-risk profile that would potentially favor implantation because it's available and on the market.

There was also a lot of specifics that may matter for particular patients, so it depends on who you are. And so what do I mean or what did our group mean when they were saying that? They were saying that depending on how high profile the individual you are versus potentially being an average citizen, that may change the benefit-risk for you of someone wanting to attack your particular device, whether you're, you know, a high-profile politician or a celebrity versus, you know, being an average person that in their mind increased your risk the higher visibility was. So if I'm an average person, it may not be something that would keep me from getting a device implanted.

Also, I would care potentially of the lifetime of my device and how likely it is that I would potentially need updates. If I'm potentially a younger person, for example, and I know that I'm going to need updates in the future, I might like the fact that my device is wireless and I may not have to come into the office and therefore be willing to accept a little bit more risk in that area for the convenience of the lifestyle that it affords me versus someone else who might be a little bit more risk averse, who enjoys going, you know, to see their physician, may be their social outlet potentially, you know, they're homebound or

otherwise.

Also they want to understand how does the device potentially fail. So if it does fail, is it catastrophic or will it default to a safe mode or some default factory settings that would influence whether I want to have the device implanted?

And they also would want the healthcare provider potentially to be able to tell them how does it compare risk to other activities that you may participate in, such as, you know, driving a car, flying a plane? So recognizing you can't quite quantify it the same way but what is the thought, at least in the sphere from the experts, about the level of risk in comparison to some activities that the patient might be able to better get their mind and their head around?

That really summarizes primarily mostly what our group talked about. So it depends a lot on personal characteristics, the faith in the FDA, and whether you can give me some essence of risk that I can understand to help me make my decision.

MR. CONWAY: Great, thank you very much. Does anyone else from Table Number 2 have any other comments they wish to provide?

(No response.)

MR. CONWAY: Thank you for your summary. I'd like to go ahead and ask the moderator for Table Number 10 to summarize your table discussion.

DR. BOCELL: Hi, my name is Fraser Bocell. I was the moderator for Table Number 10.

Question 2b: "So if yes, would you ask your healthcare provider what the alternatives are to Device C and if there are similar devices that are considered more secure?"

So there was discussion about that alternatives from treatment are part of the normal conversation with your doctor, that you should always be able to talk to your doctor

about what your choices are and about what the different risks and benefits for those choices are.

There was also discussion similar to other earlier questions that the doctor may not be the best source for this information, and especially in discussing alternatives, they may not know a lot about the cybersecurity risks, but they also might have favorite devices, ones that they were trained on, ones that they normally use usually, and so they may not be the best source of information in that.

And then in terms of what they do know about the security of the devices and about what might be more secure, we think that companies might have concerns about the unintended consequences of communications in this area, and in particular, our table felt that you really want a good source of information. And so if your provider, if your physician's not the best source of information, then it's really crucial to get a good source of information to be able to discuss or to learn about if there are better -- not better devices but other devices that would be an alternative to this, and so finding out where you could get that information where you could kind of do that research on your own.

Thank you.

MR. CONWAY: Thank you very much for your summary. Is there anyone else from Table Number 10 that has any other additional comments that you wish to provide?

(No response.)

MR. CONWAY: Great. If not, thank you. Now I'd like to go ahead ask the moderator for Table Number 4 to come up and summarize your table discussion.

DR. GEBBEN: Hello, my name is Dave Gebben, CDRH, moderator for Table Number 4.

Question 2c: "Would you want to weigh the benefits and risks of implanting a device versus managing your irregular heartbeat with medication?"

The table pointed out that one of the things implicit in that discussion is that there's

an assumption that the medications would be worse than a device if you are at the point where a device implantation was considered part of your treatment options. Along with that is that considering the risks and the benefits of implanting a device would have to be the safety, but that the safety is just another portion of the entire risks and benefits that would be part of any treatment option. They want to know and look at the totality of the appropriateness of care rather than one specific piece. As was pointed out, if you do not have a heartbeat, it doesn't really matter, but the device is rather critical, and if the security risk was such that it could be managed or taken into consideration and it was the appropriate care, then the device would be preferred to a medication.

Thank you.

MR. CONWAY: Thank you for your summary. Does anyone else from Table Number 4 have additional comments that you wish to offer?

(No response.)

MR. CONWAY: If not, thank you. I'd like to go ahead and ask the moderator for Table Number 8 to come up and summarize your discussions.

MS. CHITTOORAN: Hi, my name is Susan Chittooran, and I'm with FDA's Patient Affairs Staff. I'm the table moderator for Table 8. We discussed Question 3, which was "What would you do after seeing this information?"

So our group discussed that they would contact their healthcare provider to see if there had been any advances in cybersecurity specifically related to this device, first, since it had been implanted in the person and, two, since the vulnerability had been discovered.

Other things that were raised were one of the individuals at our table shared that they would assess the profile of the person who was doing the posting on social media to verify whether that individual was trustworthy. Other points were that we would request to see if there are any other real-world analytics or data that was able to validate the claim.

We'd reach out to other friends and contacts within the disease space, that includes support groups and patient advocacy groups, to see whether they have thoughts or experiences related to the issue that was highlighted. The group would also check the FDA website. And then, finally, the group would want to know more specifics about how it affects their device. So, for example, could this issue be disabled, and then how can it be protected?

Thank you.

MR. CONWAY: Thank you very much. At this time I'd like to ask anyone else from Table Number 8 if they have any additional comments they'd like to provide.

(No response.)

MR. CONWAY: If not, thank you.

MS. SAHA: Hello, Annie Saha, CDRH. We had Question 4 from Table Number 6, and this question was "Where would you look to find any additional information about the vulnerability concerns of those devices?"

And there was general consensus that multiple different data sources would be part of where we would look. That would include looking at the manufacturer website, but there was some discussion about that may not be the areas that you would trust and you might have some questions about the trust, but also that the information communicated on the manufacturer's site might be too complicated or too technical and so that may not be the only place.

So the FDA website would be another source of information as well as looking at hopefully that there might be news articles or other areas that might be more distilled down to get an idea of what the issue is and look at that. And it did also come up that FDA may not always be the first source, but if it came up in Google, then maybe they would go to that because Google would probably be one of the first sources.

And we also brought up the idea of cultural competencies and looking at different cultures and that people may not necessarily trust certain groups, and so patient advocacy groups and other organizations may also be a trusted source for looking at and finding information.

MR. CONWAY: Great, thank you very much. Anyone else from Table Number 6 wish to offer any comments?

(No response.)

MR. CONWAY: If not, if the moderator from Table Number 7 could approach to give your summary.

MS. MOYER: Good afternoon, my name is Vicki Moyer, and I will be reporting on the scenario regarding what if you went to your healthcare provider and asked about if your device could stop functioning due to interference from non-medical personnel.

In the scenario, the healthcare provider would confirm that it actually is possible, and what we wanted the table to discuss is what patients or the table would expect their healthcare provider to communicate to them about potential risks with this scenario, and there were a couple different perspectives at the table. One perspective was that they didn't expect the doctor or physician to communicate very much at all. This simply wasn't something that they felt the physician might be skilled in, so their bar was pretty low as far as what their expectations were for the physician to communicate about the risks if the device could stop working and what they should do.

There was an interesting suggestion about could there be a new profession emerging from these discussions today, somewhere between a cybersecurity expert, a physician, a nurse, and somewhere in the middle, somebody who's able to communicate these kinds of ideas to patients in a way that they would understand but would know enough about the devices and the technology that they could speak to it in an accurate manner and help the

physician and the community move forward with these kinds of issues that are coming to the surface.

So another scenario, another perspective was that they would want their healthcare provider to share with them about what exactly is the risk, how did they put that into perspective of the rest of their world when a patient goes to a doctor. And in these scenarios, we understand we don't know a lot about the actual probability like we do with many other scenarios. Perhaps the physician could explain it in a way of, yes, it could stop functioning, but this could also happen, and here's your options about other ways that you could think about it.

In the end, the patient would want to know what they needed to do to keep themselves safe, and then hopefully the physician would be able to explain what is the physician's role in keeping the patient safe so they could have some discussion about what this actually meant to them in a real situation.

And then another perspective was that they would like the healthcare provider to point them to the right resources. So even if the expectation was that the healthcare provider didn't have a lot of information about what they could share in cybersecurity risks, they would expect the healthcare provider to be able to point them to some resources. Some of the other questions, I think, get to some of those resources such as patient blogs with that disease or therapy was reliant on a lot of patient blogs, as some diseases are, possibly other websites, device manufacturer websites, or other kinds of trusted healthcare websites were some examples that were discussed.

Thank you.

MR. CONWAY: Thank you very much for your summary. Anyone else from Table Number 7 that wants to give any comments?

(No response.)

MR. CONWAY: Okay, thank you. Now I'd like to ask the moderator for Table Number 5 to go ahead and approach to give your summary.

MR. HAZLETT: Good afternoon. I'm Matt Hazlett, and I'm reporting for Table 5. So we were asked to answer the question of "Do you think your healthcare provider should be the main point of contact to educate you about cybersecurity risks with the device, and would you expect or want to receive information from anyone else besides your healthcare provider?"

Our table was in unified agreement that your primary care and primary decision should come from the healthcare provider for the associated device and noting that, given the scenario, that it would largely also fall to the larger device care support team and not just the primary care physician, the primary healthcare provider for the device to provide the additional support for communicating with patients reaching out for those concerns. So they would believe that the healthcare provider and the device team should be trained on the relevant information to assist in those communications, and then they'd also expect to find information available from the manufacturer such that they could point to, but they would not view that as their primary point of contact.

Thank you.

MR. CONWAY: Thank you very much for your summary. Is there anyone else from Table Number 5 that would like to give any comment?

(No response.)

MR. CONWAY: Great, thank you very much. Now I'd like to ask for the moderator from Table Number 3 to go ahead and approach.

DR. CHEN: Hello, my name is Allen Chen. I was the moderator for Table Number 3 for our question. The question asked "From whom would you expect to hear information about the safety concerns associated with Device C?" That was the first part of the



question, so I'll talk about that first.

Our group identified four major groups from which they would expect to hear information about safety concerns. Their first one was our group stated that they would rely on their physicians because their physicians would know about safety concerns due to their interactions with other patients who might also encounter these safety problems with their device.

One note that was mentioned by the group was that there might be a difference between hospital administrator and physician. Either one of these groups might be providing the safety concern information.

The second group identified was manufacturers, and the reasoning provided was that if we are able to get recall notices from an automobile manufacturer, then we should be able to get these types of notices from manufacturers. Some potential avenues that were discussed were via the UDI, or if a patient signed up for a remote monitoring app or signed up specifically to receive texts, then these may be mechanisms for identifying patients who can receive these notices.

One note that was brought up by the group is that in delivering these notices, it would be important to provide information about timing. So the message should communicate something like please contact your doctor to discuss a concern. The notice should specify whether it should be at their next routine appointment or immediately. So give a sense of timing.

The third group identified was FDA, FDA in terms of providing perhaps a warning on the device or other messaging.

And the fourth group was patient groups. Patient groups were identified as a group that would be able to more relay or channel the message rather than create the original messaging about the safety concern. The patient groups seem to be adept at collating

information so that the patient is able to get the bigger picture from the different messages out there.

The second part of Question 7 talked about what sources, including people, websites, or organizations would you consider trustworthy for relaying the safety information and recommendations associated with Device C. Again, our group identified the same groups: doctors, trusted patient groups, manufacturers, and FDA.

Thank you.

MR. CONWAY: Great, thank you very much. Is there anyone else from Table Number 3 that would want to offer any comment?

(No response.)

MR. CONWAY: If not, thank you. And now I'd ask the moderator for Table Number 11 to approach.

MS. WALLACE: Good afternoon, my name is Tammy Wallace, and I'm with the FDA. Our question was a three-part question, so I'll go over each part separately.

The first part of our question was "Do you think more routine general messaging on cybersecurity risks and safety precautions would raise awareness of cybersecurity with medical devices?"

The conversation at our table focused that routine messaging wouldn't hurt, but it would have to be organized. The device company would maybe want to spin their information, advocacy groups may sensationalize the information, and the media can definitely sensationalize the information.

It was agreed upon in the group that more messaging to educate people on how to best protect themselves is good. One problem that patients need to understand is they should not share information about their medical devices. People aren't going to hack them unless you tell them what devices you have. So don't share this kind of information online

because you could become an identified target and you must be careful about how much information you give openly about your devices.

The second part of our question was who should communicate the routine messaging. Again, the FDA and companies should educate their stakeholders and customers. General awareness campaigns are the government's responsibility, but the companies should explain how these issues are addressed when it comes to their devices. Healthcare providers should communicate this information during routine checkups, and healthcare providers should be aware of the general discussion, what the government is saying and what the company is saying.

And the last part of the question was where and what format would you expect that information. The table said they would expect to see that information through public service announcements, stories on the nightly news and morning news shows, and through technology that targets messages to individuals, such as personalized ads on websites.

And they also discussed that the format really depends on the target population. For example, for youth who don't necessarily read and have adults to take care of them, the internet may be the most beneficial place for that information. But when you're talking about the elderly who may not have access to the internet but instead watch the news, the TV is probably the most likely place to reach them.

Thank you.

MR. CONWAY: Thank you for your summary. Anyone else from Table Number 11 that would want to give any comment?

(No response.)

MR. CONWAY: If not, if I could ask for the moderator from Table Number 9 to go ahead and approach and do your summary. Thank you.

MS. NGUYEN: Good afternoon, I'm Mimi Nguyen. I was the moderator for Table

Number 9. The question was "How would you weigh the benefits of upgrading Device C against the risks of the upgrade and what would you decide to upgrade?"

So this was kind of a summary question that really went all over the different pieces, and I think our discussion at our table, a lot of the pieces that related to the benefits for doing an upgrade against this potential threat really revolved about the understanding of the exploit, so understanding the nature of the exploit, how many instances have actually happened, any kind of information to provide context to the reality that's happening to the patient to help them better understand; if this was a scenario, having a walk-through of kind of the mechanism, the complexity of the sequence of events, if you will, of how this could happen to a patient so they could truly have that information, to have that to make the benefit-risk determination.

Something else that was discussed to also help understand whether or not this is an upgrade worth doing was the lifespan of the device. A lot of implants typically are done for a certain period of time. In this part of the scenario, I believe we were past 5 years of the implant in there. So, you know, having that conversation with the healthcare provider to really understand, you know, if they don't do this upgrade and they were planning to get a new device at some point, that would be part of the consideration of the benefit-risk of doing this upgrade.

For understanding kind of the risks for that piece is really understanding the context of failure in which the device would fail if the upgrade was -- happened and really are there any other changes to the device that could potentially impact the patient.

At our table we kind of had differing opinions on kind of would the patient, would anyone decide to do the upgrade. I think the biggest takeaway from the conversation is that with the right information, they would make the upgrade assuming that the priorities of the patient and how it impacts their treatment of their disease was really going to make

that decision.

That's it. Thank you.

MR. CONWAY: Great, thank you very much. Is there anyone else from Table Number 9 that would like to offer any comments?

(No response.)

MR. CONWAY: Okay. Thank you all, the public participants in the roundtable discussions and especially FDA staff for doing a great job summarizing everything and keeping everything perfectly on time. Thank you.

At this time it's 2:30 p.m., and I'd like to go ahead and have 15 minutes of open public comments to give anyone in the audience the opportunity to provide a comment to the Committee regarding the scenarios.

Ms. Williams will read the Open Public Comment Disclosure Process at this time.

MS. WILLIAMS: Thank you.

Both the Food and Drug Administration and the public believe in a transparent process for information gathering and decision making. To ensure such transparency at the Open Public Comment session of the Advisory Committee meeting, FDA believes that it is important to understand the context of an individual's comments. For this reason, FDA encourages you, the Open Public Comment speaker, at the beginning of your written or oral statement, to advise the Committee of any financial relationship that you may have with any company or group that may be affected by the topic of this meeting. For example, this financial information may include a company's or a group's payment for your travel, lodging, or other expenses in connection with your attendance at the meeting. Likewise, FDA encourages you, at the beginning of your statement, to advise the Committee if you do not have any such financial relationships. If you choose not to address this issue of financial relationships at the beginning of your statement, it will not preclude you from speaking.

Thank you. I will now turn it back over to Mr. Conway.

MR. CONWAY: Thank you very much, Ms. Williams.

At this time I'm opening up the floor for open public comment. At the end of 15 minutes, I will close the Open Public Comment session in order to continue with the agenda. If you would like to provide a comment pertaining to the roundtable scenario discussion, please line up at the microphone. Each person, unless we exceed the 15 minutes, will be given a maximum of 2 minutes to provide a comment. Once a speaker is finished, the next speaker should immediately identify themselves and begin their remarks. I would like to ask the AV staff to please set the timer for 2 minutes for each speaker. Thank you.

(Pause.)

MR. CONWAY: It's an opportunity.

(Laughter.)

MR. CONWAY: And we do value your feedback. Thank you.

MR. HOYME: Good afternoon, my name is Ken Hoyme. I am Director for product security for Boston Scientific.

One side comment we had at our table that was related, which was as manufacturers we operate in a global environment, and so as we think about the vehicles for communication between manufacturers, physicians, patients, certainly there are privacy regulations that we have to respect within the European Union with GDPR. So some of the solutions we talked to in terms of text messages from databases, from manufacturers or things of that nature, we need to think about how we operate from a global perspective in terms of what the best mechanisms are for appropriate communications of accurate information about device security when it comes from manufacturers. Thanks.

MR. CONWAY: You're welcome. Thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Any other speakers for open public comment?

(No response.)

MR. CONWAY: Okay. To everyone who participated, we appreciate your willingness to share your perspectives with us. Your feedback today will help assure that the needs and experiences of the patients are included as a part of FDA's understanding of complex issues involving medical devices. If you didn't have the opportunity to provide a comment and you would like to do so, you may send your comment to Letise Williams at Letise, L-e-t-i-s-e, dot Williams, W-i-l-l-i-a-m-s, @fda.hhs.gov, and she will provide the Committee with your comments. Ms. Williams's contact information is also listed in the July 2nd, 2019 *Federal Register* Patient Engagement Advisory Committee Notice of Meeting. I now pronounce the Open Public Comment portion of the meeting to be officially closed.

At this point, again, thank you to everybody for your efforts through the day and the roundtable discussions. We'll now have open Committee discussion and clarifying questions from the Committee members.

As a reminder, although this portion is open to the public observers, public attendees may not participate except at the specific request of the panel Chair. Additionally, we request that all persons who are asked to speak identify themselves each time. This helps the transcriptionist identify the speakers.

So among the Committee here, are there any clarifying questions that you may have to the FDA team members and moderators on the scenario that was just discussed during that roundtable session?

My apologizes, Suzanne.

MS. SCHRANDT: Thanks, Paul.

So there might not be anyone to answer this question. It just depends on whether this happened in any scenarios, but I wondered if in the roundtable discussions did anyone

feel or surface that they are not a patient with an implanted heart device and so they weren't sure whether they would have different sentiments if they were a patient with an implanted heart device? Did that come up at all? Did anyone think maybe my opinion would be different?

DR. ROSS: Hello, my name is Astin Ross, and I'm with the FDA, and I was the moderator for Table 2. So we actually did have that discussion at our table, as well as the perspective that people also -- even if I was a patient with an implanted device, people potentially report differently than how they actually act when put into a particular situation, and so, you know, this is all perspective but that they were going to do their best to provide the information. Also recognizing that some of the people at our table came from a background that's kind of diabetes related, so they're thinking more external devices which could be a very different thing than having something that's implanted in your chest.

MR. CONWAY: Great. Any other questions?

Go right ahead, Kristina.

MS. SHERIDAN: This is a question for all tables, really. Did anybody discuss educating patients around what they should be watching for or noticing for in order to detect issues and how and when that should be communicated to the patient?

MS. SAHA: Hi, Annie Saha, moderating Table Number 6.

So it did come up in discussion that, for the physicians to really understand kind of, you know, here are the top three to five things that you should be looking out for and that should be given to the patients so that they know which things are going to be most important, that should be paid attention to rather than, you know, like a drug commercial where it has the whole litany of 12,000 different side effects that could happen, but really focus on what is the most important things. So that did come up in ours.

MS. NGUYEN: Hi. Mimi Nguyen for Table Number 9.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



We also kind of discussed a little bit about this, especially when the device is first implanted and the patient gets the opportunity, potentially, to talk to a technician about what the device is doing, to also be able to talk about kind of this, understand a little bit about the step by step of what would happen if there was a potential intrusion.

DR. BOCELL: So Fraser Bocell, Table 10.

We also discussed about being aware that there are failsafes on some of these devices, and that even if they're shut down, they'll continue to function even at a minimum level, and so knowing that would be helpful as well.

DR. CHEN: Allen Chen, Table 3.

I just wanted to add that we also talked about putting together an FAQ sheet or a website with frequently asked questions, and also discharge nurses would be an important stakeholder for providing that information or being trained. Thank you.

MR. CONWAY: Okay, great. I'll tell you what, we'll go ahead and we'll start with Bennet, Cynthia, Philip, and then Rajiv, okay?

MR. DUNLAP: Bennet Dunlap.

One of the groups mentioned assessing the risk in terms of the risks of planes, trains, and automobiles, or something like that, and I'm wondering if that discussion extended to the conversation of the risks of not having a device therapy at all and how that factored in, if it did factor in.

DR. ROSS: So Astin Ross, Table 2.

And so our group did talk about whether the device would be something that is life sustaining, so you literally, you know, need it to stay alive, or whether it's kind of a failsafe so in case something were to happen it would be able to act and that that could influence, you know, your ability to say yes or no to the device, whether it's life sustaining or it's kind of a backup.

MR. CONWAY: Okay then, Cynthia.

(Off microphone comment.)

MR. CONWAY: No. Actually, why don't we go ahead and do that now. Go ahead and turn on your microphone.

MS. CHAUHAN: My question is for Boston Scientific. I was bothered by your presentation, and I'm trying to put together why. It seemed to me that you were saying hey, wait, don't ask too much of us, we have a lot on our plate. And if that's what you were saying, that really concerns me.

MR. HOYME: Ken Hoyme.

No, that was not at all what I was intending. I was just aware that we are regulated in international environments, so solutions that can scale to all of the patients that we treat would be obviously best. Certainly, the U.S. is a large enough market that if there's a recommendation that patient databases -- so that we can communicate directly within the U.S., that's acceptable. But there are privacy rules that we have to deal with that we may end up having to create complete split solutions for the kinds of dealings.

For example, we do not have any patient identification for devices that are in cardiac patients in Europe. We have the model, serial number, and the clinic ID, and so any communication we do about a device has to go through the clinic. They understand who the patient is, we don't, where in the U.S. we have databases of patient ID cards.

So we have some of those separate solutions now, but I'm curious whether or not -- I know IMDRF has some international discussions going on about commonality of approaches and whether there's solutions that would scale globally. So no, by no means am I saying don't ask too much.

MR. CONWAY: Okay. Great, thank you very much.

Let me go ahead and come over to Philip and then Rajiv.

MR. RUTHERFORD: I heard a few different approaches to the primary point of contact questions about devices or concerns about devices. So I'm curious if any of the groups came to consensus or even had a serious difference of opinion on where the primary point of contact should be regarding devices.

DR. GEBBEN: Dave Gebben, FDA.

Our table did not have a specific discussion on the primary point of contact, but around that question we did have a conversation around the multiple streams should be in agreement so that you're hearing the same message from all stakeholders. Thank you.

MR. CONWAY: Thank you.

Rajiv.

Oh, my apologies.

MS. SAHA: Sorry, I didn't get up there fast enough. Our table did and I alluded to it -- oh, sorry, Annie Saha -- about sort of especially related to cultural and other sensitivities and diverse audiences, that it can't necessarily always be the same place, especially if you're thinking about a device that might be tracking you, that some people say if you're an illegal immigrant or something else, you may not want your data to be tracked, and so you might want to talk to other groups or like a patient group or a cultural community group rather than your physician being the main point of contact. So that was a facet that came up in our discussion.

MS. MOYER: Vicki Moyer.

Our group talked a lot throughout all the questions about how there might be a different primary point of contact depending on what the disease and the therapy was. What might be the first point of contact for a pacemaker might be different than the first point of contact for a Type 1 diabetic. That came out through all the discussions. Not only was it that I don't expect my physician to know to be my primary point of contact, but that

who would it be varied a lot. It could be a diabetes educator, it could be their primary care physician, it could be a cardiologist. It really depended on the disease and the community that surrounds the disease. That was a pretty strong theme.

MR. CONWAY: Great, thank you.

DR. CHEN: Allen Chen, Table 3.

So I just wanted to add on that I don't think we came to a consensus on one primary point of contact, but I think it was noted that the first primary point of contact -- sorry, not the first primary, the first point of contact to educate the patients should be the doctors, but the doctors should know who to direct the patients to for more specialized information. Additionally, the manufacturers should be the expert on that particular device.

MR. CONWAY: Okay, thank you.

Philip, do you feel like --

(Off microphone response.)

MR. CONWAY: Good.

Rajiv.

DR. RIMAL: So my question was very similar to what Philip asked, with maybe a slightly different focus and terminology, which is I wondered about the onus of responsibility, whether we want to call that the point of contact, maybe it's the same thing, maybe it's slightly different, because I grew increasingly uncomfortable as more and more of that onus was, I thought, being placed on the patient side. And there was one group that talked about how we're all in this kind of together, and I wondered if there was any discussion around how we think about that onus of responsibility across the entire spectrum from manufacturers on one side to patients and then the FDA and the other patient organizations on that continuum. I don't know if any group sort of thought of that onus of responsibility.

MS. NGUYEN: Hi, Mimi Nguyen from Table Number 9.

I think some of the conversations we had at our table were, you know, the onus of kind of making the fixes, too, with that interruption could be -- was on the manufacturer, it is their device. That's kind of what the conversation was, but to have those conversations with the patients and to make that benefit-risk analysis is definitely on the patient, too, whether or not it would work for them, and it was important for them for their treatment.

MR. CONWAY: Great. And one more comment in response to Rajiv, I think.

MS. SAHA: Yes. We talked a little bit -- Annie Saha, Table 6.

We talked a bit about the onus being different depending on what type of action you're really taking or what, you know, the risk of the actual cybersecurity threat is. But there was also precaution, too, about not necessarily -- that it shouldn't be all on the physicians because conversations that happen are already short enough to begin with between a physician and a patient. So adding an additional conversation on cybersecurity and the training that -- there needs to be other, sort of, failsafes and other mechanisms for that information, and the onus shouldn't just be the responsibility of the provider.

MR. CONWAY: Great, thank you.

We have two more questions up here that I can see. Three, okay. We'll go to Katherine.

DR. SEELMAN: Yeah, I was listening to this ongoing all-day problem of the confusion of not being able to ask your physician for an understanding of whatever the problem is, and one of the questions I ask myself is whether or not there was any discussion in your groups about credentialing the physician or someone else in some way, or otherwise change the policy so that there is someone else named in addition the physician. Was there any discussion in the problem of credentialing?

DR. ROSS: So Astin Ross, Table 2.

And so we weren't necessarily talking about explicitly credentialing, but there had been some discussion at our table about whether, as part of some of the counseling services that are around some of these products, particularly as more become wireless, if that should be a component of that counseling. And to the point of taking maybe some of the burden off physicians is having someone that is more in tune with both the technology as well as the health impacts that would help counsel the patient as they make those decisions.

DR. BENZ: Heather Benz, Table 1.

We also did not specifically discuss credentialing. However, the concept came up that as these issues become more common, hospitals may consider having a team that is trained not only to communicate with patients but also to advise on how the hospital deals with these things.

MS. WALLACE: Tammy Wallace, Table 11.

We, again, as the previous people indicated, didn't talk specifically about credentialing. The consensus was that the healthcare provider really should be the primary point of contact. The expectation is not necessarily that they would know everything to tell you but that they should know who to refer to you, who would have the information you want. Whether that's somebody on their staff who is more educated in the cybersecurity risks or somebody in the nursing staff or at the company, they should at least know who to refer you to.

MR. CONWAY: Okay, thank you.

And I'll ask you, Kristina, is it possible, since Mondira didn't have an opportunity this morning, Mondira, would you like to go ahead next?

DR. BHATTACHARYA: Many of you spoke about the manufacturer's website as being one source of information, but what's not clear to me is, is there a hesitation of registering

on the manufacturer's website, because that's an opportunity to get initial information when little is known but you need to be informed and then potentially follow-up information when more is known about a particular problem. Was there any discussion around the concept of registering on the site as a way of having bidirectional communication with the manufacturer?

DR. GEBBEN: Dave Gebben, Table 4 moderator.

We didn't have a discussion specifically around registration. The discussion was much more around the number and the volume of updates and notifications; we're constantly getting pinged or notified that, hey, make sure your device is up to date or, hey, make sure the security is current, or it just gets to be you see so many that you no longer pay attention.

MS. NGUYEN: Hi, Mimi Nguyen for Table 9.

We didn't talk specifically about being registered with the manufacturer, but being at our table we did actually have a couple of sponsors. So it was interesting being able to talk about how, you know, for the communication, having something verified by a third party, so similar to when you get a notification from your bank and it says verified by X. So that was something to also consider as another way to help kind of balance what that communication is about the risk.

DR. BOCELL: Fraser Bocell, Table 10.

On a related note, we talked about -- a little bit about the differences between implantable Class III devices where the company knows generally who has those in but other Class I or -- but other Class II devices where the company may not know who has their devices, and so that might be a more pertinent problem in that case where you're trying to find who has that device and who needs that alert.

MS. CHITTOORAN: Hi. Susan Chittooran, Table 8.

So our table did not talk specifically about registering with a manufacturer, but to echo one of the comments made earlier by one of the tables, we talked about being bombarded by information, but one of the interesting things that was raised was the ability to potentially opt in and opt out of the type of information you are to receive from the manufacturer so that they could decide at a later date is this information something that they would want to receive later on. So if they opt out, they would want the option of being able to go back and get that information if they need it in the future.

MR. CONWAY: Great, thank you.

Yeah, one more.

DR. BENZ: Heather Benz, Table 1.

We didn't discuss registration in particular, but did have a lot of comments at our table that the manufacturers could know the most about the device and the potential issues and could provide plain-language website information that patients could reference. We also noted that the term "firmware" in the description provided in the scenario was not necessarily plain language and might be confusing. Manufacturers would have the responsibility to communicate what they know in a way that patients can understand.

MR. CONWAY: Okay, thank you.

Now, Kristina, we'll go to you.

MS. SHERIDAN: Yes, thank you.

Was there any discussion when people -- a lot of people are saying the provider would be your first point of contact, but there's also an awful lot that's been said about the fact that a lot of providers won't necessarily know what to explain, particularly when you're comparing different devices or even a device to a medication. Was there any discussion about what sort of elements would go into a comparison framework? What would patients want to understand the comparisons between things like quality of life, things like what



would be the cost of mitigating an issue if there was an issue, things like, you know, speed of response? Was there any discussion about what would those elements be in that comparison framework that the provider would then use to communicate with their patients?

DR. ROSS: So Astin Ross from Table 2.

So we talked about that a little bit more globally, but at our table there was a lot of discussion about when you're looking at other options if you want a head-to-head comparison. So whatever you can tell me are your main selling points or areas you're going to use for that particular implantable Device C, I want to hear those same areas for any other alternative that you're going to give me.

And then we also did talk about, you know, cost and incentivizing, so both from, you know, the cost of the device itself and then going back kind of to another point about the physicians and the time, potentially looking at, you know, if there are ways to incentivize, allowing more time when those types of discussions need to take place for those higher class devices that increasingly have a lot of interconnectivity.

MS. SAHA: Annie Saha, Table 6.

We didn't go through all of the factors, but a few things that did come up were related to especially if you're talking about pharmaceutical versus a device about, you know, the potential toxicity effects over the long term, taking a pharmaceutical depending -- you know, if it's every day, the adherence aspects versus an implantable device that you have once and then it's implanted and generally should be working for a longer period of time. So that's an aspect that would be -- need to be part of sort of the shared decision-making conversation between the patient and the provider.

MR. CONWAY: Thank you.

DR. CHEN: Allen Chen, Table 3.

We didn't actually go into a framework for comparing different devices or device attributes, but it seemed that the role of the physician was to also provide kind of the clinical context and the need of the device for the patient's condition. Thank you.

MS. NGUYEN: Hi, Mimi Nguyen for Table Number 9.

So in relation to the question, the last question that we had discussed about making the benefit-risk assessment, part of it was kind of what was the most important for the patient as they are making that decision for their treatment. Is it something, you know, if it's going to be a drug, is it something I have to take every day, do I have to remind myself to use it, an alarm on my phone so I can take it every day, is that going to interrupt my way of life, compared to a device that maybe kind of you set, forget, check in with your physician every once in a while and kind of -- it comes down to kind of what is the priority to the patient.

MR. CONWAY: Thank you.

And one last comment from FDA staff.

MS. WALLACE: Hi. Tammy Wallace, Table 11.

A few things that came up in terms of how you would weigh whether you wanted to use a drug or the device, one of the biggest conversations sort of focused on insurance and the cost of the device and how a lot of times the decision isn't really up to the patient, that the insurance will tell you, you know, no, we're going to approve you to take the drug because it will delay us having to pay for the implant and the surgery for having the device implanted.

Another one was really, you know, the age of the device, as has been brought up before in this scenario, was already a 5-year implanted device. You know, if it's a 10-year normal period to have it replaced, how do you take a look at it? You know, do I go ahead and have a replacement surgery now, or do I wait until the device is up for reimplantation

anyway?

And then one of the other things was sort of looking at yourself and, you know, if you're an 89-year-old patient who has severe risks of undergoing surgery, that was something to consider whether you would opt for maybe the medical route versus having a device replaced.

MR. CONWAY: Okay. Great, thank you very much.

Was that responsive to you, Kristina?

(Off microphone response.)

MR. CONWAY: Okay. It's just about 3 o'clock. What we're going to do now is go ahead and take a 15-minute break, and then we'll be back here at 3:15. Thank you.

(Off the record at 2:59 p.m.)

(On the record at 3:16 p.m.)

MR. CONWAY: Okay, it's now 3:16, and we're going to go ahead and start here, and we'll resume the Committee meeting. At this time, let's focus our discussion on questions from the FDA. Committee members, copies of the questions are in your folder. I would ask that each Committee member identify him or herself each time he or she speaks to facilitate transcription. I would also like to remind members of the Committee that this is a general issue meeting, and reference to specific products and firms should not be included in this discussion.

I would like to remind public observers at this meeting that while this meeting is open for public observation, public attendees may not participate except at the specific request of the Committee Chair.

FDA, please read the questions. Thank you, yes. This will be Olele, Chinyelum. And you can begin whenever you want, thank you.

CDR OLELE: In general, for most safety messages (and specifically, those outside of

the realm of cybersecurity), FDA communicates the types of harms that may result from a medical device malfunction or failure and their associated likelihood of occurring, if known. Unlike other medical device safety concerns, the probability of a successful exploitation of a medical device cyber vulnerability is not knowable. This challenge can impede informed decision making between patients and healthcare providers in determining whether the benefits of a patient taking actionable steps to reduce the potential for harm (should the vulnerability be exploited) outweighs the potential risks related to deploying the cybersecurity fix (such as software updates that have a quantifiable failure rate).

- a. What approaches do you think the FDA and industry should consider in conveying cybersecurity risks to patients when the probability of exploitation is not known?
- b. Is this suggested approach similar to or different from how the FDA and industry should communicate about risks other than cybersecurity? Please explain.
- c. What additional information do you think healthcare providers should have available to aid their discussion of benefits and risks with patients?

MR. CONWAY: Great. Thank you very much. Now, before we begin this discussion, let me lay something out here for Committee members. We have five questions that we're going to discuss. You've had them in advance in your packet. You've heard the testimony this morning and also the public comments and the roundtable summaries of the scenarios. So the meeting today will adjourn at 5:30 p.m. We have closing remarks at 5:15. And so what I would ask is, as I'm trying to get a very representative opinion around the table, you have the question and we're looking for answers to this that draw on the discussion today and also the background materials. Having said that, I'll try to make certain that I get everybody in order, and if you have any doubt, put your name card up so I can clearly see you, okay?

So as we start to formulate the answer for this first question, I'm going to have to summarize back to FDA what I believe our sense of Committee is. So who would like to go ahead and begin on answering Question Number 1 or providing -- go right ahead, Necie.

MS. EDWARDS: Necie Edwards.

Question Number 1, my answer is as follows: Alert patients to some of the issues that may happen if there is a data breach, such as public service announcements on primetime news. Mailing notices should be a last resort because as we move, you may never get it in the mail, or if it is received, it may be viewed as a piece of junk mail. Also, to get community organizations involved, use radio as well as medical TVs in the doctor's office. It's just like in rheumatologists' office, when we present ourselves to the office, they have those medical TVs there. You can put this type of messaging using that type of device.

Is this approach similar? I'm going to say no. I feel it's different because I haven't seen this on primetime news.

What additional information do I feel healthcare providers should have available? Your trusted healthcare provider should take the lead and have an informational sheet available to provide to patients about the benefits and the risks. Just like the office verifies the insurance benefits and co-pays, they should be able to explain this to the patient or at least have a go-to resource for the patient. Thank you.

MR. CONWAY: Thank you.

Lisa.

MS. GILBERT: I do believe that patients should be made aware of the possibility of any malicious invention prior to the deployment of their device. Maybe comparing the risk associated with the device to something with which they're more familiar in order to give them a basis for understanding. But I think we make a mistake in saying that these risks are completely unknown and unknowable. There's a whole branch of cybersecurity whose job

is to quantify these types of risks. There is analysis available. During our training, we heard about the CVSS score, the cyber vulnerability scoring system, and I know that FDA is making an attempt to tailor that to medical devices. But those scores are readily available, and there's a handy-dandy online tool that allows us to calculate those risks. So I don't think we should think that they're completely unknowable.

And in response to how healthcare providers should communicate with patients, I really think that this is placing a heavy burden on physicians themselves. I really would like to see possibly the technician for the medical device receive cybersecurity training because I want my doctor to focus on my care and defer the technical analysis to someone with expertise in that area.

MR. CONWAY: Great.

We'll go here to Amye.

MS. LEONG: I'm actually very mixed by this simply because it's the not knowing part that my fellow colleague had just spoken about. I think that not knowing is sufficient to create fear and scare in people, and it takes just even the slightest level to create such a buzz that would be irreparable, cause irreparable harm, so I think that the harm of inappropriate, unfounded, dated information is very important. Taking a look at a particular -- I think the particularities are the most important, and you really cannot speak about all medical devices in one sentence because they're different to each type of individual, what country that you're in, each application, the installation; there are so many different things about the process of this. So I think that the FDA has to be very, very specific and go with the data. So that's the first part.

The second part is the who. My fear is -- and you know, I've gotten to know all of my medical professionals as friends. When you're at it for quite some time with the kind of diseases I had and the medical devices that I have inside of me, they are friends of the

family. I'm not so sure they're the right people to talk to me about cybersecurity in any kind of device. So, again, it depends on what the message is, and I know FDA and CDRH are very, very good, and there are templates to create the right message at the right time for the right scenario, not creating the harm but creating the good and creating the resources for people to go to, to get the right information.

So I think that the bottom line answer is it depends. It depends on what the medical device is, how much information we have, how can we gain more information about it, what is the potential threat, and move on from there. Lots of opportunities, though.

MR. CONWAY: Thank you.

Suzanne.

MS. SCHRANDT: So I couldn't agree more. I think what makes this particularly difficult is the unknown, and so my prevailing thought is when in doubt, talk to patients. And I think when we think about strategies for communication, we've already heard a lot of great, sort of, template ideas like use a yellow, red, green stoplight to signify varying levels of severity. Plain language, health literacy, those are all critical, and that should sort of be a no-brainer. Everyone should adopt those kind of concepts.

But when it comes down to an individual patient community with an individual device, I think there's really no substitute for talking to patients within that community about when is it appropriate to release a communication, what should that communication look like, not because we're experts on cybersecurity, because some of us are apparently but many of us are not; we're experts in living with these diseases and with these devices.

The critical piece here is that the time for that can't be at the moment of a threat or an issue. That relationship needs to have been established just as it is in other devices and in the drug space as well. Well, in premarket ideation, when you're first thinking about a device and the cybersecurity risks, those patient relationships should be formed so that

then it's just an iterative, continue to tap in, and you can create those communication tools and techniques together. I know that takes more time, but I really think that there's no way around that; I just think it's the smartest thing to do.

MR. CONWAY: Great. Okay, thank you.

Kristina.

MS. SHERIDAN: Yeah, I'd like to agree. That's right, the pre- versus postmarket. I think it is absolutely critical on the pre-, prior to even getting the device, that a certain level of discussion occurs just to educate patients around the particular issues that could come up so that they're not blindsided when things come. But it's not just a case of educating around the topic in general, but it's also where do you go for updates. So if something occurs, where is my go-to point to get the accurate information that will give me actionable feedback on what I can then do to help it, because that's going to inform the decision in terms of which device I go with, first of all.

For the post standpoint, for me, that becomes very critical, and it's very time sensitive. Once it's already inside me, this is where the concept of directly reaching out and understanding who has which device, if there is an ability to leverage the unique identifier, to figure out specifically where your target audience is. If the vulnerability is to a certain set of devices and I've got a different one, you're going to end up panicking me for no reason, and that fear comes into play. So this is for the post and the emergency one, having the ability to track devices down to patient level, I think, is really critical, and I know it's not necessarily there yet, but I know the mechanisms are starting to be put in place to enable that to happen in the future, and I think that's very important.

MR. CONWAY: Great, thank you.

Rajiv.

DR. RIMAL: I couldn't agree more with what was just said about the specificity of



these devices. I want to add a couple of other things. I don't think we should wait until the actual risks are known before we act because it may take a very long time to get there. But, furthermore, I'm not sure how critical that information is. There's a lot of literature that talks about presenting numeric risks that most of us cannot understand what one in a million means, but rather that there are ways of communicating about that qualitatively; that becomes more palatable to people, and for that kind of information we may not need that actual number, notwithstanding the accuracy of such numbers.

And the last thing I wanted to say was that I think in the way this question is framed and lots of the discussion today, we've spent a lot of time talking about the risks associated with all kinds of things that can happen and we said virtually nothing about the benefits of using these devices to begin with. And I think it would be doing a disservice if we only focus on one side of that pendulum without really also talking about the benefits of having that device itself. So I think it has to be placed in that context.

MR. CONWAY: Great, thank you.

Cynthia.

MS. CHAUHAN: Cynthia Chauhan.

I strongly support what you just said about risk-benefit analysis. Particularly with implanted devices, there's always risk. But the benefits often outweigh the risk. I think the first conversation about risk-benefit should be with the physician, who is your caregiver, and then the physician can choose to say for follow-up on risk, do these things, I'll get in touch with these people, I will assign these people to you.

That benefit really matters; that's why some of us at this table have implanted devices. Some of us have a number of implanted devices because we looked at the risk-benefit analysis and decided benefit outweighs risk. Do I want to know if there's risk that we did not talk about? I know there's a lot of variance on this, but I personally prefer to

know, and if I know there's an unknown risk that the professionals are considering, that helps me keep in touch with my professional about where are we on that risk and at what point does it outweigh benefit.

MR. CONWAY: Okay, thank you.

Katherine.

DR. SEELMAN: Yeah, but I'm thinking about trust. At one time we posed a great deal of trust in our physicians and the medical provider, and over time, as two skill bases began to occupy the same space, that is medicine and health on the one hand and engineering on the other, there's been a little problem about trust. We think that the M.D. may not know a sufficient amount about the technology, the devices, and the engineer, certainly about the human body and medicine.

So my point here, having seen this actually in research settings, when there's discomfort and even jockeying between medical personnel and engineering personnel, say, in telemedicine, that one simple way -- hospitals need to have a process to handle the clinical environment to make it comfortable for patients, and obviously the M.D., the medical doctor, has to know something, as Cynthia just said, and be able to be the basic platform, but then providing a trustworthy source of information for the device itself, which goes more into its efficacy, certainly at this point belongs, not perfectly, but to the people in more technical sciences.

MR. CONWAY: Great, thank you.

Any other comments on this first question?

MR. RUTHERFORD: Just one quick one.

MR. CONWAY: Go right ahead, Philip, and then we'll come to you.

MR. RUTHERFORD: I want to agree with everything that's been said about simplicity and plain language on the patient side. On the communication side, though, I was just

thinking about the way in which some devices -- and actually maybe a little bit more on the way drugs are marketed, there's a very complex and sophisticated way that companies go about weighing out a plan to market and bring products to market, and I think it would be useful in this space if something similar to that were looked at for cybersecurity risks, i.e., focus groups and testing around messaging specifically for that. I'm not suggesting there may be some organizations that are already doing that, but it feels to me like we're just in the infancy of that, and if it were possible for an organization to focus group and test this type of approach, there might be some benefit to that.

MR. CONWAY: Thank you.

DR. BHATTACHARYA: Mondira Bhattacharya.

I think it's absolutely necessary to have conversations with patients regarding cybersecurity of devices. Number one, it will give us and the patients a chance to enhance their understanding of this concept, which we've all admitted is in its infancy, number one.

Number two, I think it's a critical part of the benefit-risk discussion. So not bringing it into the choice of the device versus the side effects of the device and not having cybersecurity as an example of those potential effects would be a missed opportunity for the physician. But in terms of how to give them further information, I do think it's critical to at least have consistency in the messaging, whether you're going to the website versus speaking with your physician, because that level would otherwise create even more anxiety among some patients while others may be able to tolerate the inconsistency. So I think getting into the habit of having these discussions is part of being a healthcare provider in this era and should be part of discussing with patients.

MR. CONWAY: Great, thank you.

Any other comments for -- go right ahead, Kristina.

MS. SHERIDAN: So I just want to add one additional thing to that point. The

criticality, though, is to ensure that the providers have the information they need to share. The providers always already have a significant amount of expertise that they have to share; they're not trained as cyber experts. I would like to see manufacturers of devices have a standard set of information that has to be communicated in plain language for the providers so that they can share that information with their patients across all the devices. I think without a standard framework that allows that information to be captured from all entities that the provider can refer to, it's too much of a burden to put on them, so we have to provide help to them to provide that communication.

MR. CONWAY: Okay, great.

So at this point, Dr. Tarver, and Suzanne, what I'm going to do is see if I can go ahead and give a general belief for Question Number 1 by the Committee, and we'll see how this goes.

So in regard to the first part of the question in terms of approaches for FDA and industry and things they should consider, I'd say overall, in answer to the question, the Committee generally believes there's three strategic elements that need to be included for all three elements of Question Number 1. I'd say number one, you have to understand that the unknown is a very large factor that influences each of these subcomponents, and understanding the unknown and also the fear of the potential unknown is important to patients and consumers, that having these concerns considered, deliberated, and factored in pre-approval, well in advance, is strategic. And the other thing is understanding that there must be a balance between both risk and benefit, and especially benefit. As today's discussion kind of indicated, we're focused on the risk. Obviously, with a patient audience, many of us wouldn't be sitting here unless we had deliberated the benefits of it with our medical professionals.

But going back to subsection (a), these are some of the important elements that we

discussed. We discussed the need for all means of communications in terms of conveying risk. We talked about quantification of risk, and we also talked about the fact that particulars matter and the particulars in regard to a certain audience or particular devices and, again, the theme of balance in all things.

In the second component of this question, suggested approaches, are they similar to or are they different, you kind of have some mixed answers here. In some cases they may be similar to things that FDA currently does in terms of communications, but in other ways they may not be.

Most interestingly, I think the sense of the Committee here is that there are opportunities to explore other areas and other industries where they do communicate. I think Philip has made a very strong point here that taking a look at where the drug manufacturers are when they determine they're going to market medications to patients or different audiences, it goes through a pretty rigorous stakeholder engagement that involves not only the consumers but other factors to figure out how they would go out and message. Maybe the same type of model could be used for determining how you go out and message risk to patients.

The other concern here is where do people go for exact information or information that could be consistently updated and how is that done, and perhaps even where that is housed, whether that's government or in another type of entity.

On the third subcomponent, additional information that healthcare providers should have available to aid their discussion of benefits and risks, I think this is an interesting part here that you're hearing a very strong patient voice on. There's concern that providers are already burdened in many ways and that you have to factor in what is the burden among physicians in terms of information.

An interesting question was raised about the trust factors between physicians and

technicians, technicians meaning the technical experts who know the device well, as opposed to perhaps the prescriber or the medical professional that gives it, in reaching a balance of that. Kate has mentioned that.

I think the other thing that's been mentioned is getting the training in the appropriate place and to the appropriate person, whether or not that training and the chief messenger for that, for conveyance of risk, should be the physician or not, or should it be somebody else that's involved in the process. I think Lisa has raised that concern.

And then the other thing that has been raised is the issue of once an event does happen, how can you actually track who it has impacted, and is there a capacity there to take it to the individual patient level in terms of the notification or in terms of mitigation of risk?

The other thing, and I'll make this the final point for subsection (c), is do manufacturers actually have data that they can provide to physicians who are counseling patients or making patients aware of this, that they provide it to the physicians in advance and discuss it with them in advance so that the physician is actually talking about risk and benefit, that they're doing so with a qualified statement or qualified information.

So at this point I would ask is this an adequate response to Question Number 1?

DR. SCHWARTZ: From Suzanne, yes. Thank you.

DR. TARVER: And I agree. Dr. Tarver.

MR. CONWAY: Thank you. Then we'll go ahead and ask for the second question to be read.

CDR OLELE: In general, when FDA determines through its assessment of the vulnerability and severity of clinical impact that risks to the patient are unacceptable and there is a way to reduce those risks, the FDA will communicate. Regarding the timing of communication, the cybersecurity community holds varying views for when to

communicate risks in safety-critical industries, such as the medical device sector. A prevailing perspective to which FDA adheres is that in the absence of an effective way to reduce risk, prematurely communicating can increase the opportunity for exploitation by highlighting a potentially unknown issue and, by extension, increasing the potential exposure to harm.

A definitive fix of a vulnerability can take weeks to many months to develop and test before it can be deployed safely. While such a permanent solution (such as a software update) is being developed, risk reduction measures are recommended. It is important to note that such risk mitigations can potentially introduce other risks (such as stopping the use of a device that is beneficial to the patient), and such mitigations are often intended to only be temporary solutions (such as disconnecting from the internet).

- a. What do you think the FDA should consider as the "trigger" to communicate about medical devices affected by a cybersecurity vulnerability:
  - i. When the FDA identifies a vulnerability, even if no risk reduction measure is available;
  - ii. When there is an action for patients to take or a risk reduction measure available; or
  - iii. Other (please elaborate)?
- b. Would your recommendations change if the device was:
  - i. implanted (such as a defibrillator or deep brain stimulator),
  - ii. connected (such as an infusion pump), or
  - iii. worn (such as a Continuous Positive Airway Pressure (CPAP) machine)?

MR. CONWAY: Great, thank you.

I'll go ahead and start the response over here on my right, and we'll work around the table this way.

Free State Reporting, Inc.  
 1378 Cape St. Claire Road  
 Annapolis, MD 21409  
 (410) 974-0947

Go right ahead, Bennet.

MR. DUNLAP: Bennet Dunlap.

So one of the things that gives me pause in this is the word prematurely communicate along with safety critical industries, and I would come down on the side of more is better. And I think that it's a little paternalistic to say, well, we don't think this is going to harm, you so we're not going to communicate it, and just because I want to make Jeffrey uncomfortable, I'll suggest that there's a situation that we're all familiar with where a regulator did not act at the first warning and where they failed to inform professionals of the risk, and that was with the 737s. Pilots were reporting risks; the public didn't get it shared. That's an extreme example. It's overstating a case possibly here -- sorry, Jeffrey -- but the point is that we do better with knowledge rather than having someone make a decision for us.

So imagine you're a patient and you're considering a device. You're pretty even between two devices and you choose Device A, and then 3 months later after it's implanted, you find out that the FDA knew that there was a potential cyber risk but didn't have a solution for it, so it didn't communicate that risk and you had implanted it without knowing it. I would be pretty mad if that was me. So that's my two cents. Maybe five, sorry.

MR. CONWAY: We'll make change later.

(Laughter.)

MR. CONWAY: Necie.

MS. EDWARDS: Necie Edwards.

Fighting cyber crime is everybody's business. I view it as an obligation to do our part in the fight against cyber crime. My recommendation is there should be a trigger to establish a threshold with the vendor when a breach is actually a breach and what safeguards could have prevented a reoccurrence and once they figure out the cause of it.



Also, you could look at how many undocumented changes or attempts with the system and when it occurs.

As far as the other part of the question, whenever a provider or a vendor suggests a significant trend or a pattern that suggests a data breach, they should also be notifying the FDA immediately. Thank you.

MR. CONWAY: Thank you.

Cynthia.

MS. CHAUHAN: Cynthia Chauhan.

I agree very strongly with what Bennet said. I believe that we have a right to know even if what we know is that there's a problem for which no solution is yet available. The device is in our body or we use it, and I think that it is the responsibility of the manufacturer and the FDA to make sure that we know so that we can make choices going forward.

MR. CONWAY: Great, thank you.

Katherine.

DR. SEELMAN: I have a question, and pardon my ignorance. Are there any Level 2 and Level 1 devices that are connected devices, medical devices? We've been focusing almost completely on Level 3.

MR. CONWAY: Suzanne will answer.

DR. SCHWARTZ: Yes, this is Suzanne Schwartz.

DR. SEELMAN: Could you give us examples, also?

DR. SCHWARTZ: So infusion pumps, other types of devices that are not necessarily implanted. Currently, ventilators, other types of machines that are used for different types of interventions that are not necessarily implanted.

DR. SEELMAN: What are they, are they Level 2?

DR. SCHWARTZ: Um-hum. Yes.

DR. SEELMAN: Is there a Level 1?

DR. SCHWARTZ: So I would think that there are Class I medical devices that are connected. At the moment, there are none coming to the top of my head.

DR. SEELMAN: Thank you.

MR. CONWAY: Okay, thanks.

DR. TARVER: I'll just comment very quickly.

MR. CONWAY: Sure.

DR. TARVER: There are some Level 1 devices that may be like a vision screening tool that is a computer projection, so it is connected but it's in the diagnosis space, not necessarily in a therapeutic space, to answer your question.

I'm sorry, Michelle Tarver.

MS. GILBERT: Lisa Gilbert.

As a cybersecurity professional, my kneejerk reaction to this question was, of course, inform the patients immediately if a vulnerability is discovered. But then I talked to my daughter who is actually a patient, and she said you know there's enough stress, enough psychological burden on patients just dealing with their disease; we shouldn't unduly alarm them until there is something they can do about it. She feels that there would be a helpless feeling as far as knowing there's a vulnerability but there's nothing I can do.

And my other caution to disclosing immediately is that there are a number of bad actors out there who will take advantage of that information. As soon as they are aware of a vulnerability, they'll try to reverse engineer that to take advantage of it, so I would be really careful about disclosing too soon publicly to the wrong people. Now, I would be more than open to suggesting we disclose privately to patients but not making it public information.

MR. CONWAY: Great, thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Rajiv, did you have a comment?

(Off microphone response.)

MR. CONWAY: Okay. Philip.

MR. RUTHERFORD: Yeah, just a short comment. I think this is actually intertwined with the first question. Not having -- to your point -- sorry, Phil Rutherford. Not having an easily understood plain-language way to describe risk like the risk is similar to a plane crash or the risk is similar to a car crash or riding a bike. Yes, if every time we come up with any sort of risk we let people know that would create concern, but if we could measure, if we could figure out a way to have common language about it, then I think there would -- I think it would be okay to tell people, because I think information, to Bennet's point, information is power for the patient. So I'm somewhere in the middle on that. If we can come up with a way to effectively communicate that risk, then I think people should know, but if it's nebulous, then maybe not.

MR. CONWAY: Okay, thank you.

Kristina.

MS. SHERIDAN: Yeah, I'm definitely on the side of the patient knowing. I think it's pretty critical. When you imagine you've got kids with chronic conditions, they got devices they rely on, you may choose to make a different decision, right? So if I'm planning on going to Europe next month or I can put it off a month because of a vulnerability, I may not want to be out of the country when the resolution of the issue comes into play. I may want to -- I may make that choice or not, right?

So I think it's a couple of factors. One is what is the potential impact to the patient themselves of the vulnerability, right? If it's not going to impact my kid's health, then I may not want to know until later because it's less relevant for me. If there is a risk that it is going to affect my child's health, I want to know that so I personally can make the decision

with them in terms of do we stay within the vicinity of a hospital, within our local providers, or do we go ahead and go on vacation knowing what the situation is?

The other thing that would be critical to me is knowing when the resolution is identified and an action is something for me to take, how do I find the information, how will it get to me, and how fast can I take action when I get it. So for me, information is power, right.

MR. CONWAY: Dr. Parker.

DR. PARKER: I really agree quite a bit with what Kristina just said. I think that whether or not there is a risk reduction measure available or not, I think I would also like to know what vulnerability exists, and consistent with what Lisa said, is it something you need to, you know, broadly broadcast and that's -- the answer is no. If I'm a patient and I have a specific device, that's specific information that I need to be aware of. I don't think there's anything worse than knowing that, well, we knew this when we put this in. You knew this; you didn't tell me? I mean, that's grounds for litigation as a clinician, and you know, we're not really talking about litigation, but this is the United States of America, and we like to sue. And I think full disclosure and transparency merits that if you know that there's something likely to be wrong, whether it occurs or not, you are obligated to inform the individual. And would my recommendation change if the device was implanted, connected or worn? The answer is no.

MR. CONWAY: Okay, thank you.

Okay, Suzanne.

MS. SCHRANDT: This is a tough one because I was initially going to say I just echo what Bennet said. I think Lisa raised some interesting points, and then that's continued through, you know, through the rest of the table. I think just my inner patient advocate feels like knowledge is power, and I want to know, and yes, that would infuriate me to find

out someone knew something that they hadn't told me.

But I do think we want to be cautious about is there burden that we're creating, concern, panic, etc.? That again brings me back to it's so individualized, and I think almost in the question itself you've got an answer. An implanted device is different than a connected device, is different than a worn device because the risk profile is very different, and theoretically the diseases or the conditions those are addressing are very different, and if this is a fatal, potentially fatal almost versus something that's more of a nuisance or something like that, I just feel like it's going to be critical to understand from that patient community the mechanism for how they want to be informed, when they want to be informed, and make sure that they have the access to what they need and want.

And it goes back to that stoplight idea with the yellow, green, red. Maybe some patients who want to self-select out can just not choose to click. If they don't want to know, there's a big red alert, maybe they just don't push that button. You know, maybe we have to leave a little bit of inverse autonomy available.

MR. CONWAY: Thank you.

Amye.

MS. LEONG: Short and sweet. I agree with what -- Bennet, Lisa, Philip, Kristina? Thank you. Monique [sic] and Suzanne. And Suz has said. I think that it encompasses so many different things. There are so many different levels. This is not a uni-dimensional issue; it is 3-D, maybe even 4-D or 5-D. So it depends on so much. But I think that these kinds of considerations must be thought of with the patient at the forefront, not at the behind, as a recipient, but at the forefront.

DR. BHATTACHARYA: Mondira Bhattacharya.

I agree that patients need to be informed even before we're aware of what the solution will be or when the solution would be available, but I think the FDA needs to

develop a standardized means for that type of communication. As an example, as a physician, when I get a "Dear HCP" letter about a drug, it's very different than reading about it in the *New York Times*. The "Dear HCP" tells me a certain regulatory standard has been met and that's why I'm receiving this individualized letter. Similarly, if there are standards that could be developed for communications around cybersecurity and devices, I think patients would be less alarmed.

Two, I think besides the initial communication which should be specific to the patients who received the device, whether it's by version or manufacturer during X period, using that specificity, I think there should be an obligation by the FDA to inform when a true answer will be available, which means that the FDA needs to hold the manufacturer to providing some sort of update within a reasonable amount of time. That should be part of the original communication.

And I frankly think one of the other main reasons for telling patients is they can be monitors to see if there's phenotypic manifestation of whatever error or risk we feel has happened. So it's a lost opportunity for vigilance if we don't inform them and they continue to use the device without knowing.

MR. CONWAY: Great. Thank you very much.

So at this point, Drs. Tarver and Schwartz, with regard to Question 2, the Committee generally believes, and I'll characterize it like this, I think you're seeing not so much a dichotomy but a gradation of several things here. Overwhelmingly, I think you have a voice of patient concern and caregiver concern around this table, which is essentially a matter of principle, and the principle is this: if you know something, we would want to know it ourselves, and that involves issues of trust, transparency, and literally, I think, the credibility of an institution, of the federal government, and I think that's what you're hearing very strongly from Bennet and others.

Having said that, I think there's an issue of principle, and there are many issues of process that go along with that. I think because of that there are definite parallels to other topics that exist and are discussed in issues of security. Lisa has raised this, others have raised it during the morning, but let me go ahead and get some of these particulars out here because I think they're fundamentally important.

I think in terms of the trigger, I think, in terms of the technicalities of when you trigger, most of us would actually say at the point that there is knowledge, it should trigger something, and how you actually go about doing that comes down to the specifics, the targeted population, those most impacted, and the other specific that's involved in that is the quality and the timeliness of the data and how you communicate it. And this is very important because you can either exacerbate fear or you can help empower patients to manage a fear or an unknown so that they become more effective, and by doing so, I think one of the last points you heard here from Mondira was the fact that you might lose an opportunity to have patients as an effective part of your intelligence system, ground intelligence system for reporting back what they might be experiencing, if you can embrace them.

But I think one of the most important things is the theme of this meeting, is on communications, is a great point that Philip has raised, which is this: if we don't know how to communicate at different levels, what the risk is that you're seeing or determining or may find out or how valid the information is that you have, then it's going to be incumbent upon FDA to figure out the best way and the best types of language to alert patients, and the involvement of stakeholders in the formation of that is very important.

I think the other thing that you heard here is that in regard to the second part of the question, the implanted devices and if it's wearable or if it's connected, I think that almost became, with one exception, almost a secondary concern because the principle here is what

matters, and that's the principle of the information, in knowing at the right time.

I'd say the final note that the Committee would probably agree with hearkens back to some of the discussion that we had earlier today, which is acknowledging that in today's world there are bad actors, and as Lisa has pointed out, her profession, would definitely tell you that there are people who specifically look and monitor news to get information on vulnerabilities in order to specifically exploit them and reverse engineer, and you could inadvertently light up an area of vulnerability and risk for patients if the communications are not well thought through in terms of how you go about that. So don't leave the patient out of it, but at the same time, don't exacerbate the problem by introducing new audiences and new bad actors into the issue that you're trying to solve.

So at this point, I'll ask if that answers the question.

My apologies, go right ahead. Katherine has a question. You can go right ahead.

DR. SEELMAN: Yeah. It just occurred to me that there's a cultural aspect to this, and having just seen a movie called *Farewell*, and it's within a Chinese context, that it's the family that believes in taking on the burden of this kind of information and then doesn't necessarily share with this person who is having whatever medical problem. I think we ought to say that. And within that movie there was a recognition that U.S. usually favors giving everyone information and they can handle it, and they're suggesting that there is a cultural aspect to questions of this kind.

MR. CONWAY: I think that's an important point I'd like to add, so understanding the cultural distinctions especially in regard to communications. But at this point, I would ask is that summation adequate for you? Dr. Schwartz?

DR. SCHWARTZ: Yes, thank you.

MR. CONWAY: Dr. Tarver?

DR. TARVER: Michelle Tarver. Yes, thank you.



MR. CONWAY: Great, thank you. If I could go ahead and have the third question read.

CDR OLELE: There are best practices in cybersecurity which should be performed to maintain the security of connected devices. These include, but are not limited to: enabling, setting, and changing passwords; keeping software and applications up to date with the most recent versions; and not opening suspicious emails.

Should patients receiving new medical devices be educated about the functionality, security elements, and cybersecurity of the device, including the importance of security maintenance over the device's lifetime (often called cybersecurity hygiene) when the device is prescribed?

- a. What, if any, existing resources are available to patients to help inform this dialogue?
- b. If new resources need to be developed, who do you think should develop these educational resources (industry, FDA, healthcare systems, patient safety organizations, professional societies, public-private partnerships, or others)?
- c. How might these resources be best disseminated to attain universal patient access?

MR. CONWAY: Great, thank you. On this pass, we'll go ahead and start over on my left.

DR. BHATTACHARYA: Mondira Bhattacharya.

Well, I think we're talking about altering human behavior, which is not exactly an easy task to take on. First of all, as part of increasing the awareness of cybersecurity in the context of having a device or using a device, it's very important to provide education. From my experience in using, you know, devices in general in this multi-connected world that we live in, having something that automatically prompts you is a great way to start. Being

connected to the manufacturer's website, if it's a backup approach, if the device itself doesn't send the prompt, would be a second approach to take.

But I think whatever is developed has to be done in a collaborative fashion. For instance, if you're talking about a device in an Alzheimer's population, probably the approach needs to be different than if you're talking about someone with diabetes who's very connected on a daily basis with using their closed-loop device. So, you know, that would be my answer to this question.

MR. CONWAY: Amye.

MS. LEONG: I'll just speak to the generalities of this because I think when we look at access to the internet today, we are seeing, of course, cultural differences, we are seeing economic differences, we're seeing a large variety of just plain access issues, and then there are many other kinds of just internet hygiene, if you will, access kinds of issues. So I think that, in and of itself, even though we are not the country of the world that has the highest number of its own population with cell phones, that resides somewhere else, but people are becoming more savvy. But more savvy on a cell phone or some sort of mobile device does not necessarily mean cybersecurity hygiene.

I think the concern, for me, is about the environment in which all of this comes in. I have a mother and father who, dearly departed now, but would never learn off of any kind of mobile device. That was their generation, that was their choice, and that was respected by their children. So there are lots of differences for why people choose not to participate in that. However, now we're talking about cybersecurity hygiene as it relates to medical devices. Now we're talking about possibly my life or my child's life, and that's a whole different ballgame.

So I think that, again, like we responded to as a committee before, I hate to keep saying this, but it depends. It depends on the type of device, the interactivity of the device,

the failsafe opportunities, is it not just on and off and is that going to put someone into a defib situation? We don't know, so it depends on the specificity of the seriousness, so levels of communication that are really serious, generally important or updates are only necessary and it's automatically done for you. So where's the choice factor for the patient, and then in that choice factor, how critical is it for the person to understand that?

So I think that the FDA does have a role in that. I think that the patient and the patient population has a big role. I think that the physician and the society, the professional societies in which the physicians secure their up-to-date data in which to administer, monitor, manage, implant, remove these kinds of devices, that there is a responsibility there, as well as the patient advocacy groups for overall general patient-friendly education.

MR. CONWAY: Great. Thanks, Amye.

Suzanne.

MS. SCHRANDT: I actually just want to quickly pull through a thread that Mondira started from the last question, this idea of patients as a resource for early signaling data. We've now recognized that sort of outside of cybersecurity in the general device space. So I think when we're thinking about educating and empowering patients, particularly through patient advocacy organizations or large online communities of patients, but even at that individual level, empowering them to know their potential for that early signal information, what to do, where to go when something seems like it's not right or like it's been compromised because it's just such an important and untapped resource.

MR. CONWAY: Okay, thank you.

Okay, Dr. Parker.

DR. PARKER: Monica Parker.

There are a couple things that resonate here for me, and one of those came from a public discussion, whom do you get your safety info from; they talked about the physician,

hospital administrator, manufacturers, FDA, and patient groups, and I'd like to say that a lot of times devices that are actually inserted aren't necessarily chosen by the doctor who ends up inserting them. They are purchased by the hospital entity, right? And a lot of times the hospital entity doesn't necessarily choose what a doctor might prefer.

So when it comes to who's responsible about this, I think getting back to some of the discussion I heard a little earlier, locally hospitals, physicians, and manufacturers who sell devices to Entity A, the hospital that inserts this, I think there's a responsibility to know who got what device at what time in their facility and should be responsible for educating not only the provider, but the patients who are getting these things on a regular basis to update them. I mean, that's local. I mean, it feeds into Question Number 5, but it came from your earlier discussion.

But I think locally, if something goes bad, and I hate to be the person who brings up lawsuits all the time, but the person who is suing is going to go after the provider, going to go after the hospital and the manufacturer. So I think collectively, they have an obligation to create, let's say, a support group within a regional area to say that we inserted 150 of these devices here, we are monitoring the people within this area for problems or concerns. So I think that that is the team effort that was advocated by some of our public participants here, and I think, again, what resources need to be developed, I think that those resources need to be developed locally because the hospital knows who they're serving.

MR. CONWAY: Thank you.

Kristina.

MS. SHERIDAN: Thank you.

Yeah, in terms of should patients receiving medical devices be educated about functionality, I would say yes, as particularly around the components that the patient is responsible to take action on. So if by not taking these actions I'm going to increase my

vulnerability, I want to know that so that (a) I can protect myself or I can choose consciously to not do them knowing their vulnerability, so that's number one.

In terms of available resources, honestly, the devices I've used with my kids so far, very, very minimal information on anything with regard to the cyber components of devices. Very, very good patient direction on the use of the devices, and these are external devices, but nothing actually on cybersecurity existing that I've received.

Developing resources, I think there's two aspects of this. I think that it is important for manufacturers to have regulated standards around communications to patients, so when devices are approved, that part of the approval processes is the communication going to the patient around the patient actions that they have to take in order to maintain safety. So I think that from an FDA standpoint, I think there is an obligation to set that standard for industry, and then I think it is an obligation on industry's part to provide the information in a way that is understandable for patients to be able to follow.

To pick up on the healthcare piece of it, though, it was our home nurse who came to us and educated us on how to use that device, and so it has to be written in a language that is used by both the healthcare providers, for those who are caregivers of patients who aren't using the devices, in addition for the patients themselves who are using it.

And then in terms of the last piece (c), I strongly advocate for integrating into a device itself, if at all possible, for external devices. So if I get an email and say you have to go and do this now to your device, that's one thing. If I've got my device and something pops up and says you have to do this, just like you have a new phone today, it's far easier and quicker for me, as a patient, to follow. So, again, I'm going to push on that point of complex chronic conditions are very burdensome to manage; people often do not have time for extra stuff. So making the updates in a way that minimizes burden and number of steps and actions to take on the part of the patient is critical in order to maintain compliance.

MR. CONWAY: Great, thank you.

Philip.

MR. RUTHERFORD: Actually, reading the question, "Should patients receiving new medical devices be educated about the functionality," I wasn't aware that that was an option that they wouldn't be, like I didn't know that was a thing. And I'm not trying to be glib. I just didn't know that you could actually get a device implanted in you and not receive that information, so that's kind of scary.

I'm going to leave (a) alone and just talk about (b). If new resources need to be developed, who should develop them? The answer to that is yes, industry, FDA, healthcare, patient safety organizations, professional societies, all of the above. The question would be how do they interact between each other to develop that?

And then on (c), not just because I'm a pure advocate, but I think if you want universal peer adoption, I think the way to do that is to involve peers and specifically people that have used the devices as well. I think that's a good opportunity to leverage that tribal knowledge. That's all.

MR. CONWAY: Okay, great. Thank you.

Rajiv.

DR. RIMAL: I want to start with what my colleague, Mondira, how she characterized this as a behavior change issue, and I completely agree with that. But we also know from sort of this larger behavior change world that the best way to get people to change their behaviors is to make it easy for them to do that.

I brought this up earlier, and I'm going to bring this up again, but there's a lot of discussion here that puts, in my mind, that onus of change way on the consumer side, on the patient side, that they have to be aware, that they have to do these updates, that they have to do all these kinds of things, and less, I think, has been talked about or we have

talked less about what's the onus placed on the manufacturers and entities that are disseminating this?

So combining both of those things and bringing in this idea of choice architecture where if you make the default option the better option, the healthier option, people have the option of defaulting out of that or choosing out of that, but at least the default option is the better option, and that principle can probably be used when we think about who has that onus of change to make these changes.

MR. CONWAY: Great, thank you.

MS. GILBERT: So as a trainer, of course, I believe that all patients should be educated about good cybersecurity hygiene before they receive a medical device, along with being told about the steps that the manufacturers may be trying to take to ensure the security of their devices, so give them a little bit of peace of mind as to what the manufacturer's already doing for their safety.

Patients are already required to undergo psychiatric evaluation, at least my daughter was, before receiving a medical device, and I think a similar requirement could be made, but they need to be trained in the use of their device and in good cybersecurity hygiene and at a time when they're not under the influence of anesthesia or experiencing pain. My daughter received all of her training immediately after surgery, so of course, she doesn't remember any of it. So that is a big concern of mine, not only what they're taught but when they're taught it.

What resources are already available? I'm pretty sure, correct me if I'm wrong, that every government employee has to receive some cybersecurity training. I have to receive it annually; even though I teach it, I have to receive cybersecurity training every year. I would think that that training could be tailored, adapted to fit patients. Who should develop it? Certainly, the FDA could give guidelines as to what that training should look like. But, again,

every device is unique, so that training burden would probably have to fall on the individual manufacturers.

MR. CONWAY: Thank you.

Katherine.

DR. SEELMAN: Yes. I really think that when I wanted information for -- it's a little different in this group, I suppose. I went to the FDA's database on serious adverse events, and I think that's a very important database to further develop.

As far as the liability versus the accountability, I can draw no conclusions about that. I mean, we know that we're a litigious society, and if we can sue, we will sue, and medical professionals face this problem.

MR. CONWAY: Great, thank you.

Cynthia.

MS. CHAUHAN: Cynthia Chauhan.

I agree with much of what has been said. I particularly like the point about knowledge does not necessarily confer responsibility. I think patients have the right to know, that does not make us responsible for the devices, for the device and the outcomes. That remains with the manufacturers, I believe. I think the FDA is in a wonderful position to say this must be done in this way, and so I see them as having some responsibility for making sure that the manufacturers of the device are following through and not pushing responsibility off onto patients; it really belongs to them.

MR. CONWAY: Thank you.

Necie.

MS. EDWARDS: Necie Edwards.

As an inquisitive patient and a patient advocate, the people that I serve, we want to know when it comes down to cybersecurity in devices, we want to know what are these



changes that are being made, what's new, what has been modified for my safety, and that's very important so that you can be aware of what's new, what has been added to it.

As far as any existing resources that are available to the patients, you may be able to go to the manufacturer's website, but for many people, they may not have a cell phone, they may not have internet access. The only access they may have is if they go to their public library. When you go to your public library in order to use the computers in my community, you have to have a library card. Some people don't have a library card, which means they will not have access to that information.

In regards to Question (b), who do I feel should develop these educational resources? I feel it should be an open public-private partnership.

And (c), these resources, I feel, should be best disseminated via community health workers, support groups, patient advocacy groups as well. Thank you.

MR. CONWAY: Thank you.

Bennet.

MR. DUNLAP: Bennet Dunlap.

My colleagues have been brilliant, and I don't even have anything inflammatory to add.

(Laughter.)

MR. CONWAY: You can take another minute, if you'd like.

(Laughter.)

MR. CONWAY: So Dr. Tarver and Dr. Schwartz, with regard to Question 3, the Committee generally believes that patients, that they should be educated on functionality and cybersecurity with multiple caveats here. I think, basically, the sense of the Committee is patients are intelligent; consumers of healthcare are intelligent decision makers. However, many patients don't have access to information or the means to get it, but the

burden should not rest upon them to have to get it. We have to be creative in how to go about that. I think Rajiv made a very good point that in the dynamic of how you educate patients, perhaps using choice modeling, I think, putting forward the best choice and then having people opt out of the best choice in terms of practice is something that should be considered.

I think the overwhelming theme in terms of the general answer is that we're basically trying to determine how to change human behavior, and I think that's been stated many different times, and we all understand that's exceedingly difficult. However, given the seriousness of the topic and the need to engage all stakeholders, it's fundamentally important.

On the issue of resources that are available, you heard it overwhelmingly in here that any resources that are either existing or new have to be collaborative in terms of the development, both in terms of the message and the tone and an eye towards who will use them. I think you've seen the elevation of certain sectors, especially patient advocacy organizations have been mentioned in terms of the role that they can play in this. And in terms of who owns the resources or the development of new resources, perhaps Philip said it best, which is all of the above essentially, or yes. And I think that is true because that is the summation of everyone around the table, but that is actually how you come up with good policy and good information.

But there's some other particulars here that the Committee also generally believes, and I think Dr. Parker put a laser on one of them, which is this: Local support and local information, it goes to earlier themes that you heard about, getting information to those most impacted or those most at risk. And so what Dr. Parker outlined is local support, knowing who are these patient/consumers that might be impacted, and then how to get them aligned to resources.

I think you've also heard about the roles of professional societies, and I think you heard a good sense from the Committee here, an endorsement of the FDA's role on the landscape, that FDA plays a critically important role, because as Cynthia has pointed out, knowledge does not mean responsibility, and I think the Committee would probably agree that the only arbiter in the marketplace who can actually push industry to do the right thing at each juncture is the FDA in their role of making certain that the burden does not shift back or get placed back or by default be presumed to be resting with the patient as opposed to the industry.

One final point is that in terms of communications again, I think you see the Committee trying to figure out how to have a standard of communications that's understood among all stakeholders, but especially from the regulatory standpoint, having a standard, but also for industry in terms of their expectations on how they craft any product that they're going to use with an eye towards how it will be communicated to patients, as well as medical professionals, as well as others who are involved in the process, whether they're technicians or other types of healthcare workers.

So with that, I'll ask if that's adequate, Dr. Schwartz.

DR. SCHWARTZ: Suzanne Schwartz.

Yes, that is. Thank you.

MR. CONWAY: Dr. Tarver.

DR. TARVER: I agree, thank you.

MR. CONWAY: Great, thank you. I'll ask for the fourth question to be read.

CDR OLELE: What other recommendations do you have about the FDA's communication approach for medical device cybersecurity? How do you believe patients want to receive information about medical device cybersecurity from the FDA? Please consider each of the following:

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

- a. Designating information that is actionable versus information for awareness;
- b. Tailoring and distributing message content to multiple audiences (for example, patients, healthcare providers, industry);
- c. The format in which the information is conveyed (such as email, web posting, and social media); and
- d. Frequency with which the message is reinforced.

MR. CONWAY: Great, thank you. Go ahead and start on the right side of the table.

Hey, Bennet, here's another moment for you.

MR. DUNLAP: I think that the idea of reinforcing messages is important. I think that we all know that from watching multiple copies of the same drug ad, or they got it duct-taped, has pulled together on TV, and I think that we need to be prepared to communicate even over the risk of bad actors, and I don't just mean the guy that's duct-taped together, has pulled together, but the malicious actors already know of a potential cybersecurity vulnerability. They knew my credit card at 5:00 a.m. in the morning yesterday and used it. So they already know. I think that it's worth reinforcing, even if it's just reinforcing the idea of cyber hygiene and cybersecurity hygiene, and that's really all I have to say about it. Sorry, I can't do anything else for you.

MR. CONWAY: All right. We have one more question.

(Laughter.)

MR. CONWAY: Hey, Necie, go right ahead.

MS. EDWARDS: Necie Edwards.

Before I answer that question, briefly I would like to ask Michelle or Suzanne a question. With these medical devices, would any of these medical devices, let's say the legacy ones, would they be running older systems that may be either a Windows or a DOS base?

DR. SCHWARTZ: This is Suzanne Schwartz.

Yes, they would.

MS. EDWARDS: Thank you.

So my recommendation, one thing that concerns me is if it's a legacy device, how are they secured? Because that's going to be very important because if they're a legacy device, many of these systems are no longer being upgraded, so that is something of a great concern to me.

Now, as far as options (a), (b), (c), and (d), I would consider (a), (b), and (c), and I would like to add one to it, if I could, and that would be Webex or webinars. Thank you.

MR. CONWAY: Great, thank you.

Cynthia.

MS. CHAUHAN: Cynthia Chauhan.

My concern is around (c), the format in which the information is conveyed. I think that we rely very heavily on the internet, email, web posting, social media and that that leaves out a significant portion of our population who do not access those and we need to think about that. I happen to live in a state, Kansas, that is primarily rural with people living in very isolated situations that I think these things are not available to them. But they do receive medical care, they do receive devices, and so we need to think very carefully about how to reach that group of people and not rely too heavily on the internet type.

MR. CONWAY: Thank you very much.

Katherine.

DR. SEELMAN: I pass.

MR. CONWAY: Okay, Lisa.

MS. GILBERT: Lisa Gilbert.

I think it's really important for regular communication to take place between the

manufacturer of the devices and the patients who receive the device, not so frequent as to be irritating or nagging but with enough frequency that the patient is used to hearing from their device manufacturer so they're not going to be alarmed when they receive a communication from the manufacturer but that they'll also know to take it seriously if they have the note that this is actually important information, not just FYI.

It should be tailored to individual audiences as far as the format with which the information is conveyed. I would say exactly the same methods that are used by automobile manufacturers when they have a recall; they use postcards, they use U.S. mail, they use emails, they use nagging phone calls. My son needed his airbag replaced in his car, and the manufacturer tracked down his mother and let her know. So the manufacturers should have this information available. They should make sure they collect contact information so that they can inform their patients who have these devices.

MR. CONWAY: Okay, thank you very much.

Rajiv.

DR. RIMAL: Rajiv Rimal.

So I want to tackle that very first question, "What other recommendations do you have about the FDA's communication approach," and I want to pick up from where Lisa left off about the role of the manufacturers because I think that is absolutely critical, and what happened and what's being done seems to be central issues for the manufacturers to really tackle. So I think a communication strategy would identify what kinds of information each of the parties is responsible for. So from the manufacturers' side, I think that would be the responsibility is to say what the danger is, what has happened if some breaches happened, and what is currently to be done, and then to pass that information along. So FDA could certainly come up with and enforce guidelines on prevention, mitigation, and communication.

On the part of the providers, I think it's their role to talk about the risks and benefits of each of the devices to the best of their ability and to refer patients to other places where they can get further information.

And then on the side of the patients, what has happened, what's the risk, and specifically what is it that they need to do. We know that, as has been said before, knowledge is not behavior, but in order to have that behavior change, patients really need to know very specific things that we are asking them to undertake, which may even include advocacy for better and more secure systems.

MR. CONWAY: Thank you.

Philip.

MR. RUTHERFORD: Sorry, my head is still spinning after thinking about a medical device running on DOS.

(Laughter.)

MR. RUTHERFORD: It's truly frightening. This is just kind of piggybacking off what Rajiv said. I'm thinking back to -- and I don't know, I guess they don't use this anymore, maybe they still do and I don't remember, but shortly after 9/11 they instituted this color thing at airports, and maybe I just don't pay attention to it, so I'm not suggesting it's the most effective thing, but there was a time where when I was going to the airport, I knew if it was red I had to take my shoes off and do this thing; if it was yellow, I had to do this thing; if it was green, I had to do this thing. And I guess we talked about the stoplight methodology, but something about actionable versus awareness level and maybe something a little bit more nuanced than that. But I think, in terms of information, something like that would be very effective if we could sort of land on it and just say this is how the FDA communicates about risk and this is what it is. That's all.

MR. CONWAY: Thanks, Philip.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Kristina.

MS. SHERIDAN: Kristina Sheridan.

Yeah, to me this is very much about patient preference. If I know anything, my parents like to receive things differently than I do, than do my kids. And so the criticality for me is if I'm going to get a device and when I sign up and get that device, as I'm going through that process, I would like to be able to select the methods to receive communication that are red, yellow, or green, and for each of those things they will likely be different. And it comes down to the actionable versus awareness to me. If I have to take action on something urgently, I'm going to ask you to text me and to tell me who I need to call because I have an action to take immediately.

If it's for awareness, then I'm more likely to say sure, I can get it through an email or, you know, just ping me and tell me to go to this website to take a look at it for background information. But I want to know that up front so that I don't get that fear every time I get a message. I know if it's actionable or if it's information.

The other thing is the timeliness of this. I want to know, and this is from an experience where we have an adverse reaction and I had a child in the hospital and I was trying to find out information, and there was a voluntary recall for the stuff that was digested by my kid, and I was unable to get information on what that problem had been because it was voluntary, and I did not know where to go to get information to help my doctors find out what was going on so they could help her, and I was through this, and when you're in a crisis like that, you don't want to be on the phone calling everybody, trying to figure out what's going on. So there is the fed information, but I also want to know where do I go if something happens that is beyond the red and I haven't got a red, yellow, green to figure out if it's related to what's happening or not.

MR. CONWAY: Okay, thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



Dr. Parker.

DR. PARKER: Monica Parker.

I'm going to go back to local again. When it comes to information, manufacturers sell these devices to hospital systems and to different providers. I think manufacturers, their responsibility to the persons to whom they sold their product and to the hospitals they sold their products to, to make them aware of any changes, cyber or otherwise, and that trickles down. The persons who then inserted these devices are a local reference for the persons who received those devices from certain providers in set environments.

The other thing is, as far as the FDA is concerned, there should be a mandate by the manufacturers to keep the FDA, I guess, alerted about the cybersecurity issues, and if manufacturers are not responsive, to recall the product so they can't sell it anymore.

The other thing is that providers who are inserting these devices, we talked about training and credentialing; there needs to be an annual update or awareness of what needs to go on with a device, A, B or C, whatever that is, and that training should be given annually, or there should be an update of some sort, and you can give the learner that training however that learner chooses to get it, whether it's through webinars, web posting, however it is they get continuing education units for the professional community. And, again, I think that the professionals who are responsible, getting back to that team, can locally inform people who have those devices.

And then the frequency with which a message is reinforced, I think annually, through continuing educational events, whether locally, regionally, or nationally, we have a responsibility to get these updates. But I think there's a regulatory function for the FDA, and if the manufacturer is not updating and making sure that the providers who have been trained -- because before these devices are inserted, people are trained on them, usually by the manufacturer.

MR. CONWAY: Great. Thank you very much.

Suzanne.

(Off microphone response.)

MR. CONWAY: Okay, Amye.

MS. LEONG: I think for me it's ditto on what everyone has said so far. I think the role of FDA is truly the standard setter. But it's not just setting the standard but holding and being even the enforcer of those standards with manufacturers. And I think that those companies that make these devices have to be held, they should be held accountable. How they then distribute it through other health delivery systems, hospitals, individual providers or whatnot, it is still their device.

And I'll be honest with you, and these are joint replacements, so they're not interactive, but only with the sense that they interact with me, is that I was never told or never given any owner's manual on joint replacements. When I moved, I never had any sense of responsibility to alert my orthopedic surgeon or have I ever received an alert from any orthopedic surgeon, and I'm the UN spokesperson.

But, anyway, so it's quite frightening, you know, when someone like me is so readily available with metal parts in her body in a lot of different places that I'm not even getting alerted to any particular updates over a long period of time. So, certainly, the responsibility, as I see it, as a patient, is with the FDA to set that standard to the manufacturers and set it in a way that there are actionable items, as has been discussed by my fellow Committee members, but also that there's an enforcement, a very strong enforcement factor.

MR. CONWAY: Great, thank you.

Mondira.

DR. BHATTACHARYA: Mondira Bhattacharya.

I agree with most of what's said, just a couple of things to reinforce. I think when someone receives a new device, it's important to perhaps tailor the frequency to more frequent at the beginning and then annual after, especially if it's going to be a chronic use device, to better reinforce the necessary concepts, and I think it is critical. We heard this morning from our engaged audience that they often receive a lot of information from manufacturers, so it is very important to distinguish new important information from routine education; that's a principle that should be employed not just in cybersecurity but in all aspects of use of the device.

MR. CONWAY: Great, thank you.

Let me come back to you, Kristina.

MS. SHERIDAN: I just want to add one point on the last bullet, the frequency of the message. We haven't talked about a closed loop yet, so if I get any text and I've got something that I need to reply to, say yes, I've read it, I've got it, then you know I've received it. Even on informational messaging, if I don't reply and say I've received it, maybe I'll get a follow-up a week later. But I think if we can include that closed-loop mechanism, we'll avoid alert fatigue.

MR. CONWAY: Okay, great. Thank you.

Drs. Tarver and Schwartz, with regard to Question Number 4, the Committee generally believes (1), overwhelmingly, I think you heard a reaffirmation of the role, purpose, and importance of FDA in using their authority as an honest broker in the system to look out for patients but also to maintain standards of high accountability for manufacturers, both to patients and to healthcare systems. Dr. Parker has talked about this twice now, in particular, not only in terms of how it impacts people, but also hospital systems and in healthcare delivery systems, that theme has occurred over several different questions. But I think, in particular, on this one it's vitally important.

In terms of some of the components of the questions here, this issue of what's actionable and what's for awareness, it's a complex question in issues of security and homeland security and national security, but there are two major things that go along with that. Number one, if you're identifying something as actionable, the basic human question of therefore then what do you do and where do you go for the information.

The other thing is the gradation or the stratification of what is the issue, and this is something that Philip and others have hit on in terms of the stoplight or the red, yellow, green. And while that was derided, this is my personal comment, while that was derided many times after 9/11, the fact is it did provide clarity in a moment of crisis over a period of time that conditioned the public to understand what certain types of information meant at certain periods of time, and I think that's been raised several times around the table that that type of distinction by FDA based on threat or based on what information they're handling is of importance so that people can actually understand it and how to react.

In terms of the tailoring, I've touched on that a bit. There are many different audiences here, understanding who those audiences are. I think that Cynthia has put her finger on a very important point, it's in the summary document and it's also been a longstanding concern of FDA and to start with, that's the population, whether the young, old, socioeconomic factors, rural, but those people who are not online, the people that we might miss in immediate communications. And the people that may actually be missed even by manufacturers of devices who may not be actively seeking out or might find it too cost prohibitive to try to get that information, you're hearing a very clear sense that we have to be able to be flexible enough to communicate with all recipients of devices on what the risk is even if they're not connected.

Really, that kind of gets to the issue that many of us were talking about here in terms of answers, that the tactics matter as much as the principle of being timely in

communications. So of the tactics that were listed, others were added to it including Webex, which is important, but again I think that a high standard of outreach to all patients regardless of what means and access they have to communications.

The other thing, there have been several analogies that had been raised about planes and cars. And I think they're good, you know. I think you might want to take a look, as FDA, at some of the high standards that the Department of Transportation has in its different agencies where they hold manufacturers to very high standards across the supply chain and also by means and methods of travel, including mandates that they have for communications to passengers. That might be on there, or carriers of those who use those types of communications, I think there might be some examples there.

On the issue of frequency, I think that based on the expertise around the table, you're hearing a couple of different things in terms of certification, whether that's annual, but also you're hearing a very strong sense, again based on expertise, that there's a conditioning that takes place with certain target populations that you're trying to impact where the more they see information that's coming in, the more they may get used to the fact that it's important to pay attention to it and then you can probably taper off from there.

But, again, on a final note in regard to all the elements of this question, I think you're hearing an overwhelming sense from this Committee that the purpose, the role, and the relevance of FDA is probably more timely than ever, especially in their role as being a strong hand in the marketplace to protect the consumer and also to make certain that those manufacturers of devices own the device, get the device approved, and then if they're seeking payment for that device, they understand that throughout that process, they own it thus they have the majority of the responsibility.

So I'll ask you at this time if that is an adequate summation.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

Dr. Schwartz?

DR. SCHWARTZ: Suzanne Schwartz.

Yes, that is. Thank you.

MR. CONWAY: Great.

Dr. Tarver?

DR. TARVER: Thank you.

MR. CONWAY: Great. If I could ask for the fifth question to be read.

CDR OLELE: Hard-to-reach populations include those in rural or other areas with limited access to health care providers or facilities, or limited access to the internet and other wireless technologies.

- a. What do you recommend the FDA, patient organizations, industry and health care providers do to disseminate information about medical device cybersecurity issues to these populations?
- b. What other organizations or groups could partner with other stakeholders to facilitate communication with these populations?
- c. Who is responsible for ensuring hard-to-reach patients receive the messages?

MR. CONWAY: Thank you. So we'll go ahead and start. We'll start over on the left.

DR. BHATTACHARYA: Mondira Bhattacharya.

This is such an important issue in healthcare in general. One way to approach this is analogous to what was done with blood-borne pathogens training in the early '90s for those of you that were around in healthcare then. I mean, literally, patients were being sort of targeted as being potentially HIV positive, and people were taking precautions when handling them as opposed to ignoring it for other patients.

This was after a few nosocomial episodes of HIV had occurred. It became a public health concern through the Joint Commission, through the CDC, through local health

societies, through medical schools, through disease state organizations. We were all educated, every level of healthcare, private offices, academic medical centers, large hospital associations, community health clinics, and that's how the behavior was changed. The appropriate precautions were taken not because you thought a patient was infected but because you knew you had to protect yourself if you were coming in contact with blood, period. Took a few years, and now any new medical student is equipped with this information.

So this is that important. It's really necessary to introduce those concepts into the curriculum of pharmacy schools, nursing schools, medical schools, dental schools. Work through the disease state organizations like cardiology, endocrinology, nephrology earlier, the ones that actually use devices a lot more than let's say my field of infectious disease. So starting in a targeted fashion, it's really important to introduce this concept because we heard from our audience of the three different places they go for information: they first go to their healthcare provider, whether it's an M.D. or not an M.D.; then go to the FDA because the FDA approved the device and they have trust in the FDA. So I would start with the healthcare system and introduce this education widely, with FDA being one of the governmental sponsors of this public health effort.

MR. CONWAY: Thank you.

Amye.

MS. LEONG: I think we're all singing the same tune here, at least the two of us are. I see the FDA as the area from which push occurs, that information is pushed through in a templated form with the standards piece to this. When I say plain English, almost a visual English, if you will, rather than plain English, so that people of all colors, all cultures, all ages have a sense of it.

Mondira talked about the HIV piece, and when she and I talked about it earlier, I said

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

you know, I actually remember when Dr. C. Everett Koop sent a letter to every single household in the United States. Some of you may not even remember that, but that was such a unique scenario. It was not a scare tactic. It was done with love, with care, with great information, with tremendous resource, resources available as well as -- it was a hard copy letter, so you can imagine the resources available to even do that in this day and age. But it can be done, but it did take years to really change movement and beliefs.

I think people who live in hard-to-reach areas or not accessible by any cyber anything, there are advocacy groups, there are hands-on-the-ground people who are working in the communities to assist, and not utilizing those currently existing social and health services would be a disservice, I think, and a misuse of valuable resource for the FDA.

MR. CONWAY: Great. Thanks, Amye.

Suzanne.

MS. SCHRANDT: Yeah. So like Cynthia, I'm also a Kansas girl. I lived there most of my life, and I'm from there, so it's funny to think about rural folks as hard to reach. I think of them more as differently reached, and I think we have to go find them where they are.

There's a famous PCORI funded study in Colorado looking at Colorado ranchers, and they had very low rates of colonoscopies, and so a researcher was interested and said why is that? So it turned out the ranchers didn't want to talk about it, it was embarrassing, so they put advertisements on cattle auction bid sheets, and it drove rates up, and they made them kind of funny. I won't repeat them here, they were crass given the subject matter so I won't repeat them, but they worked.

And so when you think about where are people going to get data, get information in a rural population, farm bureaus, rural assistance centers, area agencies on aging, faith-based communities, churches, and the FDA can tap into the national sort of organizations, National Rural Health Association, there's the Faith and Opportunity Initiative at HHS, and I



think there's some partnership up, up top, and then at the bottom, and then to echo Amye's sentiment about patient advocacy organizations have far-reaching tentacles. They usually have local, you know, organizing forces on the ground, so I think they're certainly not unreachable. We just have to be kind of creative.

MR. CONWAY: Great, thanks.

Dr. Parker.

DR. PARKER: Monica Parker.

Having practiced in a rural area, I agree with much of what has been said. I do believe that local people go to local places. They do go to their hospitals first; they do go to their doctors first; they do go to the public health department because that's frequently the only primary care provider in most communities. So where do you go? You go where you receive your healthcare.

If you want to increase awareness in more rural areas or hard-to-reach areas, if you will, local radio, public radio. I know for the African-American community there was a consumer study that showed that most people get a lot of their health information from the radio or they're prompted to get information elsewhere by getting it from the radio first.

Other organizations or groups (b) that could partner with other stakeholders to facilitate communication with these populations, insurance providers. And who is responsible for ensuring hard-to-reach patients receive these messages? Unfortunately, it's always going to be the providers and the hospitals. I think if you're in crisis in a small town that's like 500 people, you're not going to call the FDA.

MR. CONWAY: Thanks, Doctor.

Go ahead, Kristina.

MS. SHERIDAN: Kristina Sheridan.

Again, I think it comes to patient preference. If we're talking about specifically rural

patients who have medical devices, they received the device somewhere. At the time they receive it, if they can specify their preference for receiving information, that closes that gap rapidly, right; they get it by the same means just like -- well, through their choice.

A couple of other thoughts I do have is that device manufacturers, when they submit their device and they're looking for information of what they can put forward, I hope we ask them what their plan is for communication to all patients, not just rural versus urban but those with, you know, less than grade eight education levels or English is not their first language, so asking those questions of manufacturers so that they can pre-think that and have a plan and looking at what that is and making sure it's acceptable to some kind of standard, I think, would be very beneficial for this also.

And I think there are certain things if you're rural, you really are not connected. Maybe some of the training information, for example, around staying secure can be put onto videos that they can re-watch when they need to re-watch. If they forget something about how to do it, they have it available locally to them and it's not just streamed. So having local resources, I think, is important to leverage in community care organizations. And then the post office is still the one agency that touches every house, so that is always your fallback.

MR. CONWAY: Okay, great. Thank you.

Philip.

MR. RUTHERFORD: I agree with my colleagues. One thing -- Phil Rutherford.

One thing with section (b) in organizations -- and I think of hard-to-reach populations as both Flint, Michigan and rural Kansas, both hard-to-reach populations. Community health workers or community workers, period. Even in rural communities there's someone; there's a country doctor, there's someone that is seeing to the health of that community. There's usually an opportunity to connect with them and get some information and share

some information.

MR. CONWAY: Great, thank you.

Rajiv.

DR. RIMAL: I would just say all of the above, that these communication modalities are not one or the other, and the more urgent the matter, the more redundant the channels need to be.

MR. CONWAY: Great, thank you.

Lisa.

MS. GILBERT: I don't really have anything to add. I think all of the suggestions that have been made are excellent. I may be unique in having grown up in Niobrara County, Wyoming, which is the least populous county in the least populous state in the Union, and one observation that I would make is those folks are not very likely to come under cyber attack honestly. If they have a connected medical device, if they're in Niobrara County, Wyoming, they're not going to be connected, they're not going to come under attack. So I guess maybe that gives Cynthia or other Kansans and Wyomingites a modicum of comfort. They really are not at as great a risk simply because they are hard to reach; they're also hard to reach by attackers.

MR. CONWAY: Great.

Katherine.

DR. SEELMAN: Yes. This is kind of a nice way to get to the end of things, to bring up the social justice question here, which essentially it is and it always will be. Agreed that rural areas are not wired, and also in my career, the same question has come up about how do we bring this technology to rural areas.

So having started my career as a community organizer, both rural and urban, before I got into these more complicated careers, I agree that on a local level there's a lot of

resources that have to be connected to somebody. I don't know if there's such a thing as a registry at the Level 3 level of connected devices, but we use it in other areas. For example, in research we certainly have registries for high-level quadriplegics who are using, say, very complicated mobility devices which, in themselves, are communication devices. I don't know if there's the capacity for monitoring if you have the names of people who use these devices.

And finally, as I said before, some consumer case studies would be very interesting to see what the life of what they're doing, how they're handling it themselves and that would bring us some more information about them, and I doubt if these kinds of case studies -- so I certainly would be interested in the case studies. Thank you.

MR. CONWAY: Sure.

Cynthia.

MS. CHAUHAN: Cynthia Chauhan.

I appreciate Lisa's comfort. I worked in, in the '80s and the '90s, in HIV through public health, and I think that we should really consider close alliance with public health in rural communities because community health workers are there and the public health departments usually administer the federal programs that go into these communities, so they would be a very good partner for working together to make sure that whoever is using these devices in the communities is safe and is connected.

MR. CONWAY: Thank you.

Necie.

MS. EDWARDS: Necie Edwards.

I agree with everything that was stated. I just would like to add two things. One, in a rural community, some of these communities do have mobile health units on wheels where they do travel to the population. The second thing that I would like to add is one of

the government payers users CCM, chronic care management. If something similar could be done where the physician, if you know that you have a patient that's on a device, depending upon your patient load, do something similar to what is done with CCM where you're picking up the phone, actually calling the patient, having a 20-minute or less conversation with that patient to update them and keep them abreast. Thank you.

MR. CONWAY: Okay, thank you.

We're running a little bit ahead here, Bennet.

MR. DUNLAP: I hate to ruin your expectations. I'm going to be quick. Philip, thanks for reminding us that Flint matters as much as rural Kansas. I think that's an important point. I think it's also likely that all of these communities will become increasingly connected, so I look forward to the auction ads about cybersecurity, even if they are the kind of thing that would appeal to my sense of humor.

MR. CONWAY: I'm a trained auctioneer, so we could have a little fun, Bennet.

(Laughter.)

MR. CONWAY: Great. Thank you very much.

So I'll pose the question now, after I do a quick summary here. I think basically what the Committee would conclude at this point for Question Number 5 is, one, I think we would all agree we've given you a pretty rich tapestry of tactical and practical that you can draw from on the transcript. I think some of them may not occur to folks that regulate; I think things like the U.S. Postal Service touches everybody's life, public health workers. Some of these are actually entities that are factored into other federal agency protocols in the event of emergencies and for information distribution. You might want to talk to some of the other federal agency partners that you have in terms of distributions that the other agencies may be charged with for information.

But I think there are a couple of major things here that have been stated: (1) the

importance of timely communications; (2) a proactive view of pushing the message out using all factors; (3) I think the Committee would say that we're in agreement that FDA has many different powers. We talked about the powers to regulate, but also FDA has the power to convene, and whether that's in person or online, you have the power to convene many of these different stakeholders to talk about tactics and things that would be best for them to take on in terms of distribution of methods.

I think there's been a lot of discussion about rural populations, hard-to-reach populations. Just as importantly, I think we had a pretty well-rounded discussion of things that are or should be displayed visually and not just in terms of language, and I think probably earlier today you saw some of that in the expert testimony and the public testimony of using visual displays for information.

I think of all the different tactics and all the different platforms that were talked about, I'm not putting words in the mouths of my Committee members here, but based on a former life, there's a saying in public communications and mass communications that redundancy is a good thing across as many channels as possible to the targeted and intended audience as frequently as possible, involving as many different letterheads. So not just FDA but other trusted letterheads in that local area gets a higher result. The prospect of registries was also raised, and I think that's good. I think overall, in terms of strategy, we have to understand that we're tackling something that's relatively new in some sectors. Some sectors have not invested that much capital or resources or attention in the issue of cybersecurity, so taking a look at things like curriculum, taking a look at things where content is communicated and planned for the long term, utilize all stakeholders.

A couple other quick points here: Again, the Committee has sent a very strong signal to FDA that how you approach manufacturers and the expectations you create for manufacturers on how to communicate to all patients regardless of where their station is in

the country or in life or socioeconomically, they should come to you with a plan for how you folks define patient populations and then let them stand up to the plate and describe that to you.

The last point that I'll make here is the issue of patient choice, and I think Kristina has hit on this several times as have others, that you have to be able to, at the front end, provide information to patients so that they can opt in or understand how they can get communications in a timely manner on those issues that might impact them the most. So if there's a device that's been hacked or something that's been compromised, that's an immediate thing. If there's a general concern, they know how to get that, but the patient is put in a role of picking the means of communications, if it's coming from an official source or if it's coming from a manufacturer.

And one other thing that was mentioned in regard to this question that I think is timely and that we can all draw from, look at the lessons of the 1980s and the work that patient advocates, that community workers, and community healthcare workers and, in fact, many federal agencies, especially FDA, look at the tactics and the time that was used and invested to educate specific populations with HIV or AIDS and those groups that were working with them on how they could best communicate. I think there are a lot of lessons from history that are probably still applicable there.

So, at this point, I'll ask you is this adequate?

Dr. Schwartz?

DR. SCHWARTZ: Suzanne Schwartz.

Yes, it is. Thank you.

MR. CONWAY: Dr. Tarver?

DR. TARVER: Michelle Tarver.

I appreciate the comments, thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

MR. CONWAY: Thank you.

I'd like to thank the Committee and the FDA for the contributions. I'd also like to thank the Open Public Hearing speakers, industry, medical professionals, patient organizations, research organizations, and the FDA for their remarks.

I'd ask, at this point, the FDA representatives sitting at the table if they have any concluding remarks, either Dr. Tarver and Dr. Schwartz.

DR. SCHWARTZ: Thank you.

So yes, on behalf of FDA, I want to thank also all the members of the Patient Engagement Advisory Committee here today and the Chair, Paul Conway, for the insightful discussions, the critical insights that you shared with us today. I'd also like to thank all of the invited speakers as well as those who provided comment during the Open Public Hearing session and, finally, to all of our FDA staff who supported today's meeting serving as moderators during the roundtable discussion and to Ms. Letise Williams, the PEAC Designated Federal Officer.

You know, communicating on cybersecurity risks of medical devices is a challenging topic, and it's an endeavor that is indeed in its infancy at present. At FDA we've underscored the very nature of cybersecurity being ever evolving, particularly as we approach this from a policy perspective. Communicating around cybersecurity risk is really no different. It's going to have to be iterative. It's in its infancy at present, and we really appreciate all of the important contributions and insights that you shared with us today. We look forward to digesting and synthesizing all of this important information and then determining what those next steps will be. And make no mistake, we'll be reaching back out to this Committee as we progress for your continued feedback and direction. Thank you for helping us fulfill our public health mission.

MR. CONWAY: Thank you.

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947



Dr. Tarver.

DR. TARVER: So I just want to echo our gratitude to the Committee for its insightful comments, for its thoughtful responses to our questions, and we really will plan to take this back under consideration. As Suzanne already alluded to, we plan to continue this dialogue, and we appreciate you all's commitment to public service by helping the FDA.

MR. CONWAY: Thank you.

I'd like to thank you all for joining us at the third meeting of the Patient Engagement Advisory Committee where we, the patients and care partners, provide our perspective to FDA's Center for Devices and Radiological Health, CDRH. Your participation today will be an initial step in helping to assure the needs and experiences of patients are included as part of the FDA's communication approach for medical device cybersecurity. We ask that you consider completing the survey shown at the link on the slide or the hard copy that was provided so that we can get your feedback on this meeting and inform how we conduct future meetings.

One final point, I usually don't offer too many personal perspectives as the Chair, but I will say this. First, I think hats off to the FDA for the work that was done well in advance, years in advance of this meeting, and for your ongoing engagement with patients. As a patient and as the former president and now the chair of policy for a national patient organization, access, sensitivity, listening, and following through is a hallmark of CDRH, and I personally appreciate it. I know my fellow Committee members feel just as strongly, that this experience is substantive and worthwhile; it's public service, but most importantly, it's service that helps you get your mission done.

I'd also like to say this, that we are on the eve of September 11th, we're on September 10th, and if you go back and take a look at the import of the September 11th Commission, there's an interesting sentence in there, and to generalize it, it basically says

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947

what did we suffer through and what did we go through. We went through the failure of imagination. And to the staff who worked on that report and to the principles that were involved in it, that was a very important point to raise, and I think it's relevant to this.

I think that FDA and I think patient advocates and I think national security practitioners are all aware of the different risks that the United States confronts. For patients who depend on lifesaving medical devices, we depend a lot on the FDA, but the truth of the matter is that those who are accountable for patients and patient safety is a very wide ecosystem including manufacturers, and what I hope is that this discussion and this transcript is used in the future so that people have a point of reflection and they think to themselves what are we not imagining, because you've heard several folks at this table talk in terms of how do you not simply target one patient but how could you actually go to a class of patients?

And I would say that in terms of FDA, I applaud your efforts to work collaboratively with other federal agencies including DHS, the DoD components that are relevant. But, again, for your public service, for the leadership, and for the rank-and-file civil service, we understand that those who serve America are serving patients, and in regard to cybersecurity, you are an extension of our protection, and we appreciate it. And thank you very much for having this meeting. It's with gratitude. Thank you.

(Whereupon, at 5:14 p.m., the meeting was adjourned.)

C E R T I F I C A T E

This is to certify that the attached proceedings in the matter of:

PATIENT ENGAGEMENT ADVISORY COMMITTEE

September 10, 2019

Gaithersburg, Maryland

were held as herein appears, and that this is the original transcription thereof for the files of the Food and Drug Administration, Center for Devices and Radiological Health.

---

TOM BOWMAN

Official Reporter

Free State Reporting, Inc.  
1378 Cape St. Claire Road  
Annapolis, MD 21409  
(410) 974-0947